AUTOMATION

User Manual

UM EN RAD-80211-XD...

Wireless Ethernet Radios
802.11 Transceiver Series

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATION

User Manual
Wireless Ethernet Radios 802.11 Transceiver Series

04/2009

Designation: UM EN RAD-80211-XD...

Revision: I

Order No.:

This user manual is valid for:

Designation	Version	Order No.
RAD-80211-XD		2885728
RAD-80211-XD-BUS		2885757
RAD-80211-XD-WM		2885715

Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this manual.

User group of this manual

The use of products described in this manual is oriented exclusively to

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER
This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION
This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

The following types of messages provide information about possible property damage and general information concerning proper operation and ease-of-use.

NOTE
This symbol and the accompanying text alerts the reader to a situation which may cause damage or malfunction to the device, either hardware or software, or surrounding property.

This symbol and the accompanying text provides additional information to the reader. It is also used as a reference to other sources of information (manuals, data sheets, literature) on the subject matter, product, etc.

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of legal authority

This manual, including all illustrations contained herein, is copyright protected. Use of this manual by any third party is forbidden. Reproduction, translation, and public disclosure, as well as electronic and photographic archiving or alteration requires the express written consent of Phoenix Contact. Violators are liable for damages.

Phoenix Contact reserves all rights in the case of patent award or listing of a registered design. Third-party products are always named without reference to patent rights. The existence of such rights shall not be excluded.

Modbus is a registered trademark of Schneider Automation. Wi-Fi is a registered trademark of the Wi-Fi Alliance.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:

www.phoenixcontact.com.

Make sure you always use the latest documentation. It can be downloaded at:

www.phoenixcontact.net/download.

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary. Subsidiary contact information is available at www.phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
Germany
Phone +49 - (0) 52 35 - 3-00
Fax +49 - (0) 52 35 - 3-4 12 00

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to

tecdoc@phoenixcontact.com.

Table of Contents

1 802.11 Series Overview 1-3

1.1 Basic Features of the IEEE 802.11 Wireless Standards 1-3
1.2 Radio Descriptions 1-4
1.3 Wireless Standard IEEE 802.11 Basics 1-8
1.4 Access Point/Client Configurations 1-9
1.5 Bridge Configurations 1-9
1.6 Data Encryption and Security 1-11
1.7 SSID (Service Set ID) 1-11
1.8 Access Point and Client Encryption 1-12
1.9 Bridge Encryption 1-13
1.10 DHCP Server 1-13
1.11 Operator Authentication and Management 1-14
1.12 Modbus/TCP I/O Emulation 1-14
1.13 Ethernet Terminal Server 1-14

2 System Planning 2-3

2.1 Accessing the Site 2-3
2.2 Path Quality Analysis 2-3
2.3 Signal Strength 2-3
2.4 Antennas and Cabling 2-4
2.5 Antenna Mounting Considerations 2-6
2.6 Maintaining System Performance 2-7

3 Installation 3-3

3.1 Mounting the Radios 3-3
3.2 Making Connections and Powering Up 3-8

4 Programming the Radio 4-3

4.1 Configuring the PC to Communicate with the Radio 4-3
4.2 Logging Into the Radio 4-3
4.3 Viewing Device Information 4-4
4.4 General Device Information 4-5
4.5 Local Diagnostics 4-6
4.6 General Configuration 4-7
4.7 Operational Mode 4-8
4.8 LAN Configuration 4-9
4.9 SNMP Configuration 4-10
4.10 DHCP Server 4-11

4.11 Configuring the RAD-80211-XD... as an Access Point 4-12
4.12 Client Configuration 4-21
4.13 Bridge Configuration 4-25
4.14 I/O Ports 4-31
4.15 Passwords 4-34
4.16 Store and Retrieve Settings 4-35
4.17 Performance 4-36
4.18 Maintenance 4-36
4.19 Monitoring/Reports 4-38

5 XD-BUS Configuration for I/O Modules (RAD-80211-XD-BUS only) 5-3
5.1 I/O Communications 5-3
5.2 I/O Module Descriptions 5-8
5.3 Addressing the Remote I/O 5-9
5.4 Rotary Switches 5-15
5.5 Register Scaling 5-15
5.6 Wiring and Fail Condition DIP Switches for the I/O Modules 5-18
5.7 Accessing the XML file 5-28

6 Radio Troubleshooting 6-3
6.1 LED Indicators 6-3
6.2 RSSI (Received Signal Strength Indicator) 6-5
6.3 General Troubleshooting 6-7
6.4 Resetting the IP Address 6-9

7 Technical Data 7-3
7.1 RAD-80211-XD and RAD-80211-XD-BUS 7-3
7.2 RAD-80211-XD-WM 7-4
7.3 Dimensions 7-5

8 Ordering Information 8-3
8.1 RAD-80211-XD and RAD-80211-XD-BUS Parts and Assemblies 8-3
8.2 RAD-80211-XD-WM Parts and Assemblies 8-5
8.3 Additional Parts and Accessories 8-6

A Technical Appendix A-1

A 1 Structure of IP Addresses A-1

A 2 Assigning IP Addresses A-1

B Appendices B-1

B 1 List of Figures B-1

B 2 List of Tables B-5

B 3 Explanation of Terms B-7

Section 1

This section informs you about

- Basic features of IEEE 802.11
- Access point/client configurations
- Bridge configurations
- Data encryption and security availability
- SSID
- Modbus/TCP I/O emulation
- Ethernet Terminal Server

802.11 Series Overview 1-3

1.1 Basic Features of the IEEE 802.11 Wireless Standards 1-3

1.2 Radio Descriptions 1-4
- 1.2.1 RAD-80211-XD 1-4
- 1.2.2 RAD-80211-XD-BUS 1-5
- 1.2.3 RAD-80211-XD-WM 1-7

1.3 Wireless Standard IEEE 802.11 Basics 1-8
- 1.3.1 802.11b 1-8
- 1.3.2 802.11a 1-8
- 1.3.3 802.11g 1-8
- 1.3.4 802.11b/g Mixed 1-8

1.4 Access Point/Client Configurations 1-9
- 1.4.1 Example of Access Point/Client Topologies 1-9

1.5 Bridge Configurations 1-9
- 1.5.1 Point-to-Point Bridging 1-10
- 1.5.2 Point-to-Multipoint Bridging 1-10
- 1.5.3 Repeater Mode 1-11

1.6 Data Encryption and Security 1-11

1.7 SSID (Service Set ID) 1-11

1.8 Access Point and Client Encryption 1-12
- 1.8.1 WEP Encryption 1-12
- 1.8.2 WPA with TKIP/AES-CCMP Encryption 1-12
- 1.8.3 MAC Address Filtering 1-12

1.9 Bridge Encryption 1-13
- 1.9.1 AES 1-13

1.10 DHCP Server 1-13

1.11 Operator Authentication and Management 1-14

1.12 Modbus/TCP I/O Emulation 1-14

1.13 Ethernet Terminal Server 1-14

1 802.11 Series Overview

1.1 Basic Features of the IEEE 802.11 Wireless Standards

The Phoenix Contact RAD-80211-XD... radio transceivers are capable of transmitting Ethernet data using transmission methods conforming to IEEE 802.11a/b/g standards. This manual describes the RAD-80211-XD, RAD-80211-XD-BUS, and RAD-80211-XD-WM radios.

Each radio can be programmed to function as an Access Point, Client or a Bridge. Some of the features of this series include:

– **802.11i Security:** This algorithm provides an exceptionally high level of security that is currently deemed unhackable.
– **Local and Remote Diagnostics:** An RF link dry contact provides local assurance of link between radios. The RSSI test point provides an easy way to check the strength of the RF signal. Advanced diagnostics are available via the web-based management.
– **RS-232/422/485 Serial Ports:** Two built-in serial ports allow the transmission of serial data using the 802.11 wireless protocol. Ethernet and serial data can be sent simultaneously.
– **Adjustable Transmit Power:** Ability to raise or lower the power level to reduce the RF range to facility boundaries or boost it to overcome obstructions in the path.
– **Logging and Reporting Capabilities:** Logs can be kept of any configuration changes, attempts to gain access to the network or which clients are connected.

CAUTION:

Important Notice (RF Exposure)

Installation of this transmitter system's antennas must be performed in a manner that will provide at least a 2 m (6 ft.) clearance from the front radiating aperture to any user or member of the public.

This product is intended for fixed installation applications.

FCC Part 15 Compliance

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by Phoenix Contact will void the user's authority to operate the equipment.

FCC Part 15.247
ISC RSS 2101

1.2 Radio Descriptions

1.2.1 RAD-80211-XD

The RAD-80211-XD is a DIN rail-mount radio with a protection rating of IP20 (see Figure 1-1). This radio features an RJ45 connector for connection of Ethernet devices as well as an RS-232 and RS-422/485 port, which gives it the capability of sending serial data to another transceiver over the 802.11 radio link. The RAD-80211-XD features an RF link dry contact for indicating a radio link and an RSSI (Received Signal Strength Indicator) voltage test point to aid installation and troubleshooting. There are two (2) antenna connectors for antenna diversity.

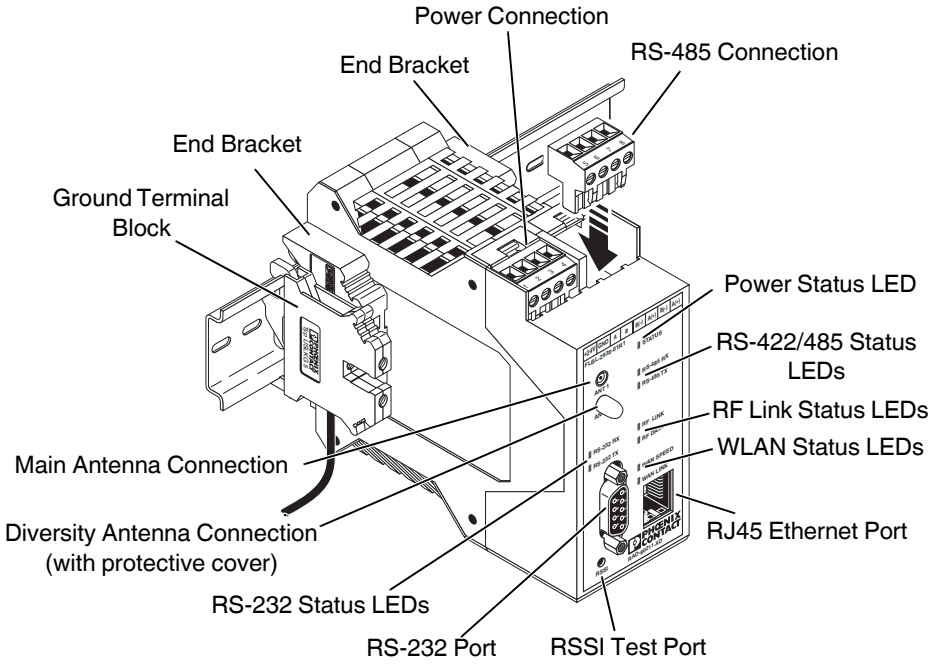


Figure 1-1 Features of the RAD-80211-XD wireless radio

1.2.2 RAD-80211-XD-BUS

The RAD-80211-XD-BUS radio differs physically from the RAD-80211-XD in that it has a 5-pin BUS connector on the side of the unit (see Figure 1-2). This BUS connector is designed to allow analog, digital, or frequency input/output modules to be connected (see Figure 1-3). It also has a Modbus/TCP Gateway and an Ethernet Terminal Server. The I/O modules are accessed using Modbus/TCP protocol through an access point or a bridge radio (gateway). The I/O values are also available for read-only applications via an embedded XML file.

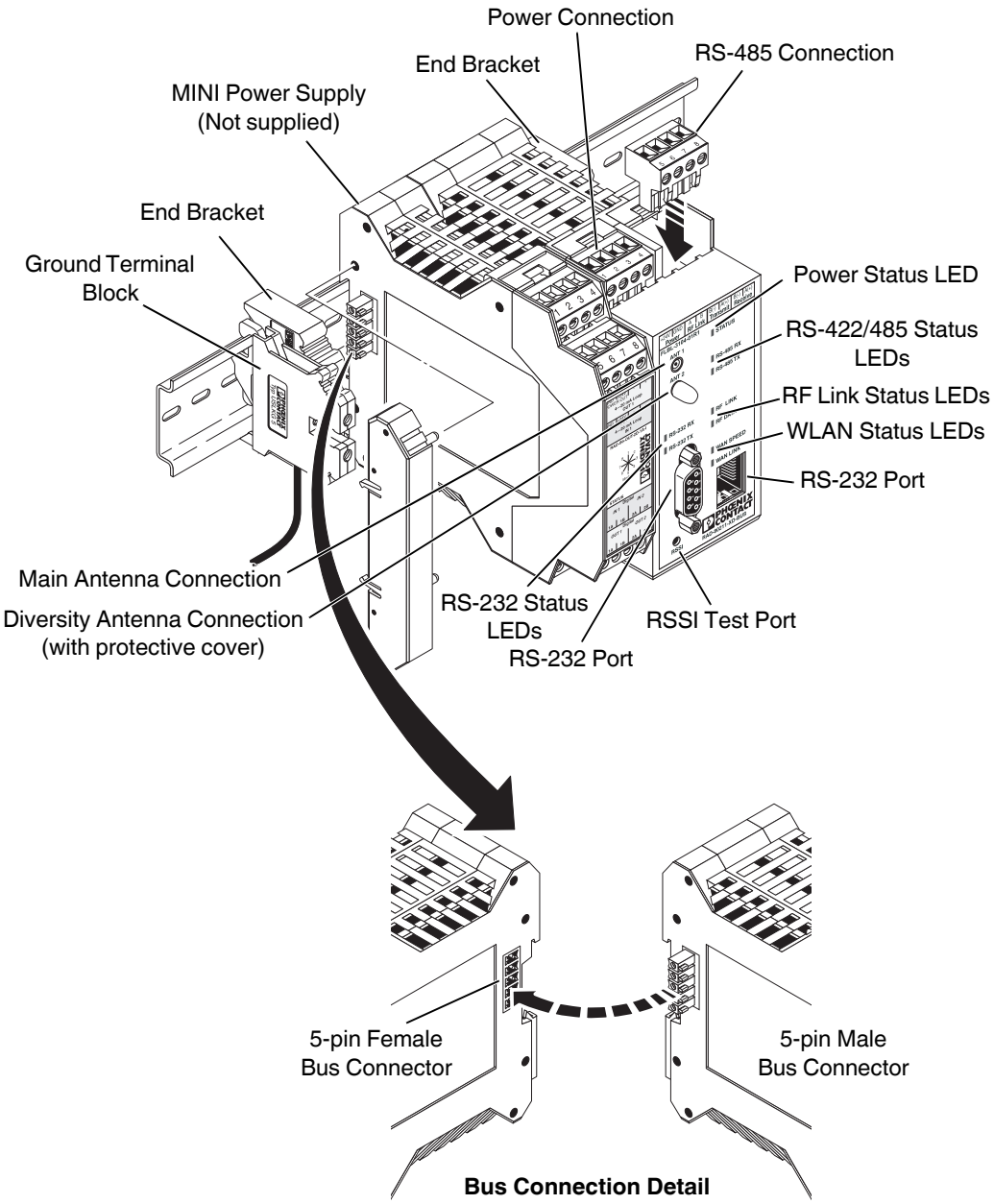


Figure 1-2 Features of the RAD-80211-XD-BUS wireless radio

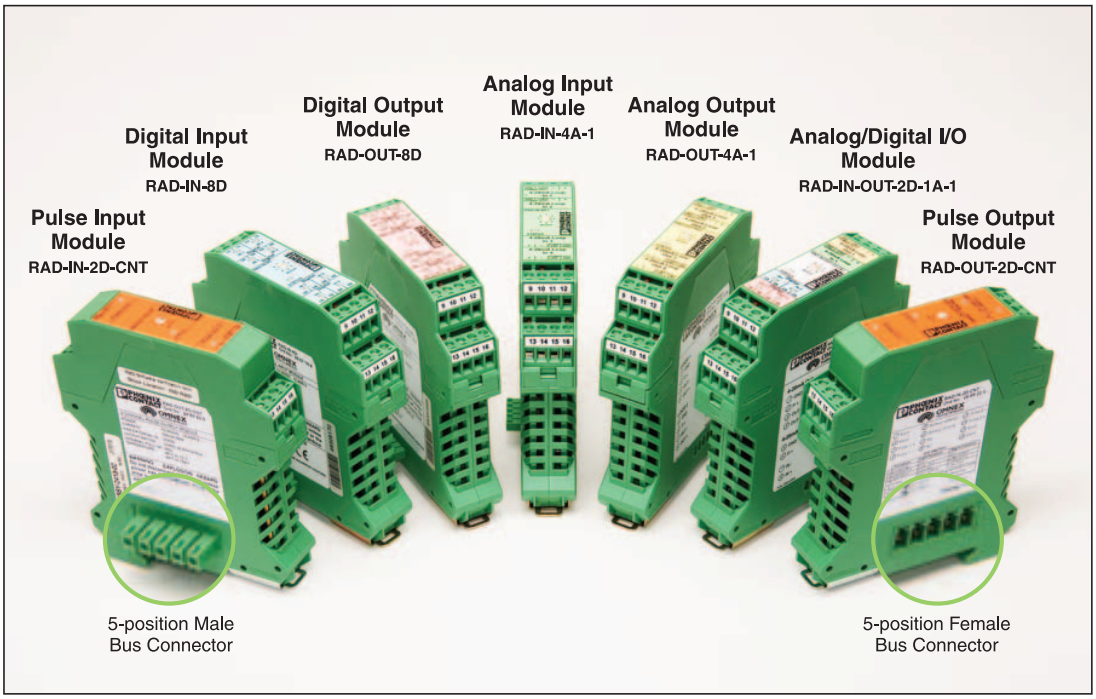


Figure 1-3 I/O Modules used with the RAD-80211-XD-BUS

1.2.3 RAD-80211-XD-WM

The RAD-80211-XD-WM (see Figure 1-4) is a wall-mount radio with IP54 protection for non-hazardous locations. This radio features splash resistant connectors for the connection of Ethernet and RS-232 and RS-422/485 devices. It can be powered via a standard power supply or Power-over-Ethernet (PoE). The RAD-80211-XD-WM features an RF link dry contact for indicating a radio link and an RSSI (Received Signal Strength Indicator) voltage test point to aid installation and troubleshooting. The RAD-80211-XD-WM radio comes with two sealed antenna connectors for antenna diversity.

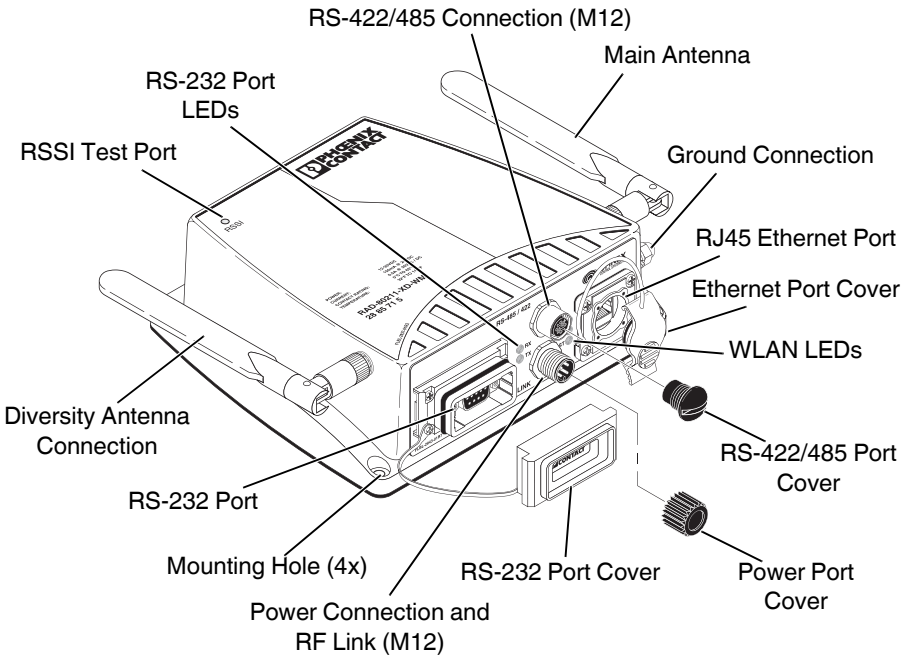


Figure 1-4 Features of the RAD-80211-XD-WM wireless radio

1.3 Wireless Standard IEEE 802.11 Basics

1.3.1 802.11b

The IEEE 802.11b standard, developed by the Wireless Ethernet Compatibility Alliance (WECA) and ratified by IEEE, establishes a stable standard for compatibility. A user with an 802.11b product can use any brand of access point with any other brand of client hardware (or bridge to bridge) that is built to the 802.11b standard for basic interconnection.

802.11b devices provide up to 11 Mbps transmission speed, and can fall back to 5.5, 2 and 1 Mbps depending on signal strength or user selection. The 802.11b uses DSSS (Direct Sequence Spread Spectrum) and operates in the 2.4 GHz band.

1.3.2 802.11a

The IEEE 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5 GHz band. 802.11a uses OFDM (Orthogonal Frequency Division Multiplexing).

1.3.3 802.11g

802.11g operates at data rates up to 54 Mbps within the 2.4 GHz band using OFDM. 802.11g is backwards compatible with 802.11b.

1.3.4 802.11b/g Mixed

802.11b/g Mixed mode only applies to access points and allows both 802.11b and 802.11g clients to connect using optimum settings.

1.4 Access Point/Client Configurations

A transceiver configured as an access point can only communicate with devices configured as clients. A transceiver operating in bridge mode can only communicate with other bridge mode devices.

All wireless devices connected to the access point are configured on the same subnetwork as the wired network interface and can be accessed by devices on the wired network.

1.4.1 Example of Access Point/Client Topologies

An access point can be used as a stand-alone access point without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices (see Figure 1-5).

The RAD-80211-XD... radios can be used as one of a number of access points connected to an existing Ethernet network to bridge between the wired and wireless environments. Each access point can operate independently of the other access points on the same LAN. Multiple Access Points can coexist as separate individual networks at the same site by using different SSIDs and operating on different channels. It is recommended that non-overlapping channels be used to minimize interference.

The most common configuration is multiple access points connected to a wired network in various locations to provide a wider coverage area. This enables wireless client devices to roam freely about a site switching from access point to access point. The access points all have the same SSID but operate on different channels.

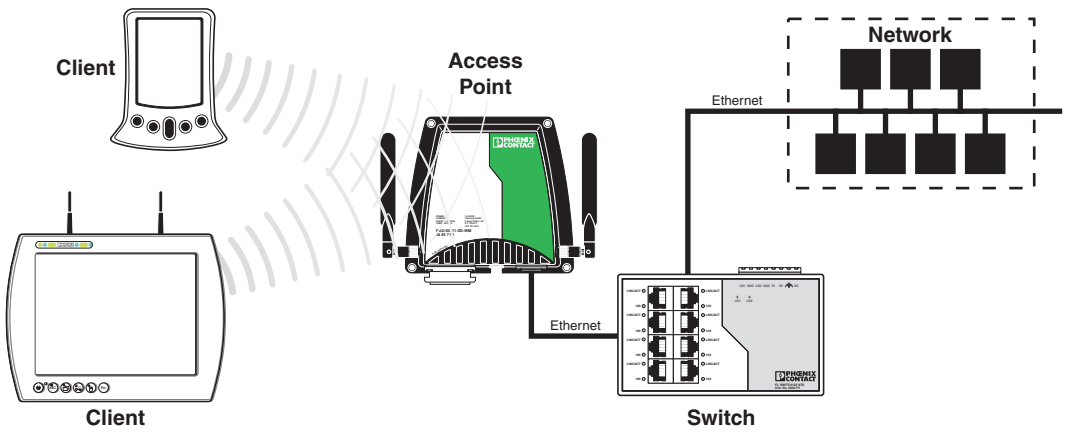


Figure 1-5 Example of Access Point/Client

1.5 Bridge Configurations

The wireless bridging function of the RAD-80211-XD... supports several different configurations. The most popular ones are described below.

1.5.1 Point-to-Point Bridging

Figure 1-6 shows Point-to-Point bridging of two Ethernet links.

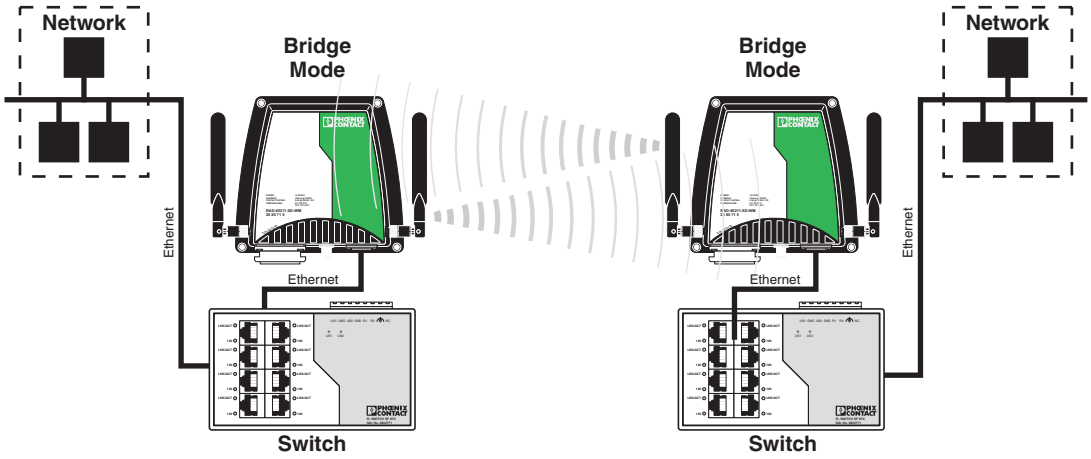


Figure 1-6 Example of Point-to-Point Bridging

1.5.2 Point-to-Multipoint Bridging

Figure 1-7 shows Point-to-Multipoint bridging of multiple Ethernet networks.

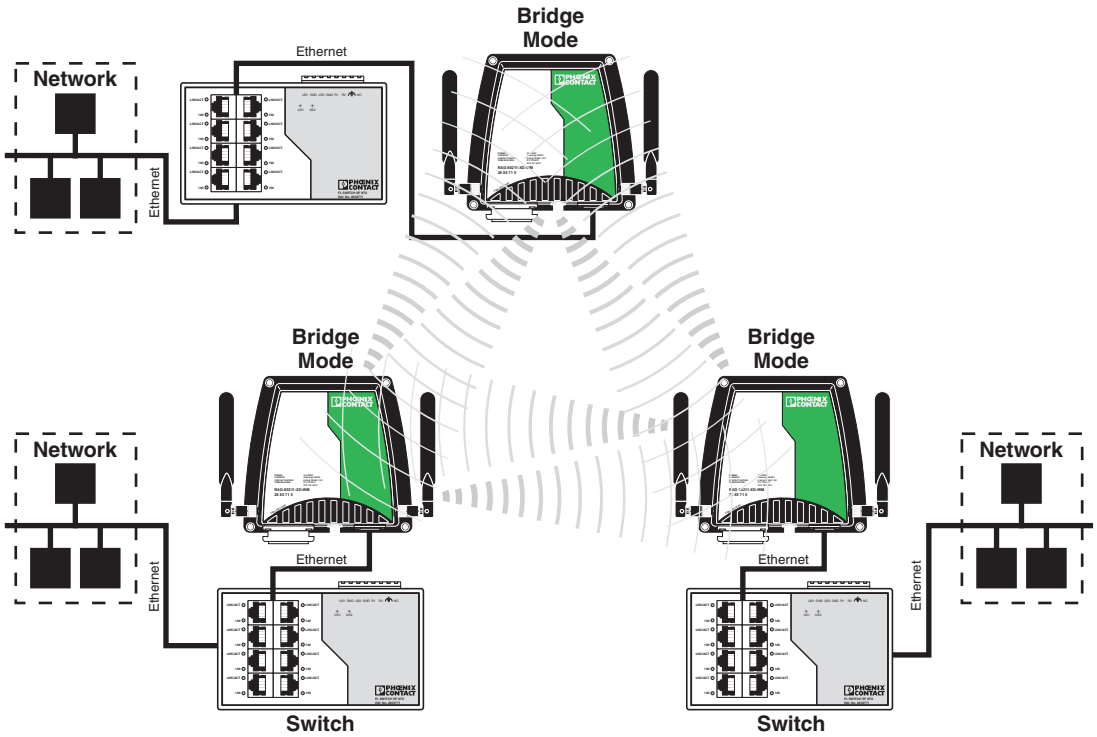


Figure 1-7 Example of Bridge/Repeater Mode

1.5.3 Repeater Mode

Figure 1-8 shows three radios all configured as bridges; two are connected to LAN networks, and the third simply acts as a repeater to extend the range.

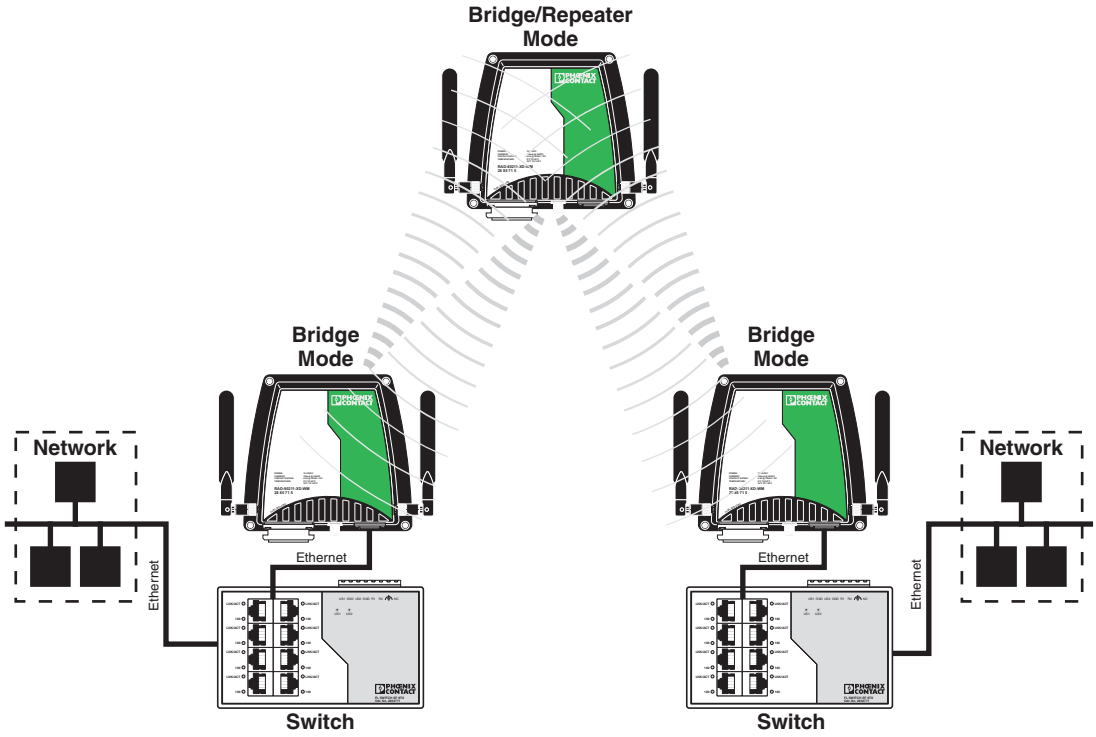


Figure 1-8 Example of Point-to-Multipoint Bridging

1.6 Data Encryption and Security

The RAD-80211-XD... radios feature several advanced security technologies. Access points and clients can be operated using no security (not recommended), WEP, WPA™ or WPA2™ (802.11i). In Bridge mode, no security or AES encryption can be used. Some level of security is recommended.

1.7 SSID (Service Set ID)

The Service Set ID is a string used to identify a network among multiple wireless access points. The SSID can act as a basic password without which the client cannot connect to the network. Choosing to broadcast the SSID allows any client to discover the access point. Disabling SSID broadcasting is the most basic form of wireless network protection.

1.8 Access Point and Client Encryption

1.8.1 WEP Encryption

WEP (Wired Equivalent Privacy) encryption is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP relies on the use of identical static keys deployed on client stations and access points.

There is also shared or open authentication that applies to WEP. When shared authentication is configured, the access point performs an additional step when a new client is first detected. The access point sends out an authentication request to the client. The client then encrypts the request using the WEP key it has, and sends it to the access point. The access point then confirms (or denies access) that the new client has the correct WEP key. When open authentication is configured, this step is skipped. Data being sent back and forth is still encrypted using the WEP key.

Utilities exist for monitoring wireless traffic encrypted using WEP. After a certain amount of traffic has been monitored, these utilities can recognize encryption patterns. Additional security should be used such as hiding the SSID and MAC address filtering. This will create a network with a minimal level of security; however, it is not suitable for sensitive data.

1.8.2 WPA with TKIP/AES-CCMP Encryption

Wi-Fi Protected Access or WPA was designed to enable use of wireless legacy systems employing WEP while improving security. WPA uses improved data encryption through the temporal key integrity protocol (TKIP) which mixes keys using a hashing algorithm and adds an integrity-checking feature to ensure that the keys haven't been tampered with. TKIP also incorporates re-keying, so the key is periodically changed to prevent old keys from being captured and used for unauthorized network access.

In addition, user authentication is enabled using the extensible authentication protocol (EAP). Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. It can also employ a form of AES (Advanced Encryption Standard) called AES-CCMP.

AES-Counter Mode CBC-MAC Protocol (AES-CCMP) is an encryption algorithm used in the 802.11i security protocol. It uses the AES block cipher, but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point.

AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

1.8.3 MAC Address Filtering

The MAC (Media Access Control) address is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the MAC layer. The MAC layer interfaces directly with the network media. Consequently, each network device requires a unique MAC address.

Authentication is the process of proving a client's identity. The RAD-80211-XD, RAD-80211-XD-BUS and RAD-80211-XD-WM can utilize MAC address filtering to detect an attempt to connect by an unauthorized client. The transceiver will compare the client's MAC address to those on a user predefined MAC address filter list. Only client addresses found on the list are allowed to associate. MAC addresses are preassigned by the manufacturer for each wireless card.

1.9 Bridge Encryption

1.9.1 AES

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES is currently approved for military use, and utilizes a 128-bit block cipher algorithm and encryption technique for protecting computerized information.

The RAD-80211-XD, RAD-80211-XD-BUS and RAD-80211-XD-WM are compatible with networks that use a Dynamic Host Control Protocol (DHCP) server for allocating IP addresses. In addition, an access point can be configured to function as the DHCP Server for a network.

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the RAD-80211-XD family of radios requires that you enter an ID and password. The factory defaults are:

The user name and password are case sensitive.

A. Access to Configuration options

For access to configuration options, use the following log in:

– User name = Admin
– Password = admin

B. Access to Monitoring Screens

For access to monitoring screens only, use the following log in:

– User name = Monitor
– Password = monitor

1.10 DHCP Server

The RAD-80211-XD, RAD-80211-XD-BUS and RAD-80211-WM are compatible with networks that use a Dynamic Host Control Protocol (DHCP) server for allocating IP addresses.

In addition, an access point can be configured to function as the DHCP Server for a network.

1.11 Operator Authentication and Management

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the RAD-80211-XD family of radios requires that you enter an ID and password. The factory defaults are:

The user name and password are case sensitive.

Access to Configuration options

For access to configuration options, use the following log in:

– User name = Admin
– Password = admin

Access to Monitoring Screens

For access to monitoring screens only, use the following log in:

– User name = Monitor
– Password = monitor

1.12 Modbus/TCP I/O Emulation

One RAD-80211 radio must be selected to function as the Modbus/TCP Gateway. All RAD-80211-XD-BUS radios in emulation mode will function as Modbus slaves. If the network consists of access points (AP) and clients, the access point must be the Modbus/TCP Gateway and the clients will be Modbus slaves. If the network consists of bridge mode radios, only one bridge can be programmed to function as the Gateway. All other bridges must be slaves. Any of the I/O ports on the radios (including the RS-232 and RS-422/485 ports as well as the expandable I/O modules) can be connected together via the two serial channels. This means that a slave PLC can be connected to either serial port of a radio, in addition, analog, digital and pulse/frequency I/O modules can be attached to the BUS connector of the RAD-80211-XD-BUS.

1.13 Ethernet Terminal Server

The Ethernet Terminal Server mode allows serial data to be encapsulated and transmitted over Ethernet. In access point/client topology, the access point must have the Ethernet Terminal enabled. If the network is in bridge mode, then only one bridge can have the Ethernet terminal enabled.

Serial data packaged within TCP or UDP protocol is sent from some device and received by the radio acting as the Ethernet terminal. The Ethernet terminal strips off the TCP/UDP protocol headers and sends the serial data out on one of the serial streams. The wireless link then distributes this data to all other radios' serial ports connected to that serial stream. If the serial protocol is addressable (e.g. Modbus, DF1, etc.), the end device will ignore any data that is not addressed to it.

Section 2

This section informs you about
- Site assessment
- Path quality analysis
- Signal strength
- Antennas, cabling, and antenna mounting considerations
- Maintaining system performance

System Planning 2-3

2.1 Accessing the Site 2-3

2.2 Path Quality Analysis 2-3

2.3 Signal Strength 2-3

2.4 Antennas and Cabling 2-4

2.4.1 Coaxial Cable Considerations 2-5

2.5 Antenna Mounting Considerations 2-6

2.6 Maintaining System Performance 2-7

2.6.1 Antennas and Coaxial Cable 2-7

2.6.2 Cable Connections 2-7

2.6.3 Power Supply 2-7

2 System Planning

2.1 Accessing the Site

To achieve the best radio performance possible, the installation sites have to be given careful consideration. The primary requirements for a reliable installation include:

– Antenna placement that allows for line-of-sight or adequate signal strength
– Primary power source that provides required current
– Protection of radio equipment from exposure to weather or temperature extremes
– Suitable entrances for antenna, lightning arrestor, interface or other required cables - if using remote antennas.

These requirements can be quickly assessed in most applications. A possible exception is the first item, verifying that a clear line-of-sight exists. A non-obstructed path is ideal; however, minor obstructions in the signal path will not always block communication. In general, the need for a clear path becomes greater as the transmission distance increases.

2.2 Path Quality Analysis

With the exception of short-range applications, a path loss study is generally recommended for new installations. The exceptions include distances of less than 92 m (300 ft.) where no test is required in 90% of applications, and where a test is done with a functional Phoenix Contact radio set to the desired wireless mode (802.11a, b or g), transmit data rate and transmit power setting. However, where towers would need to be built just to do the test, a path loss study is more practical. A path loss study predicts the signal strength reliability and estimates the fade margin of a proposed radio link. While terrain, elevation and distance are the major factors in this process, a path loss study also considers antenna gain, coaxial cable loss, transmitter power and receiver sensitivity to arrive at a final prediction.

Path loss studies are normally performed by a communications consultant, wireless hardware vendor or a system integrator who uses topographic maps or a software path analysis to evaluate a proposed path.

Although path studies provide valuable assistance in system planning, they are not perfect in their predictions. It is difficult, for example, to consider the effects of man-made obstructions or foliage growth without performing an actual on-air test. Such tests can be done using temporarily installed equipment.

2.3 Signal Strength

The strength of radio signals in a well designed radio network must exceed the minimum level needed to establish basic communication. The excess signal is known as the fade margin, and it compensates for variations in signal level which may occur from time to time due to foliage growth, minor antenna misalignment or changing atmospheric losses.

While the required amount of fade margin differs from one system to another, experience has shown that a level of 20 dB above the receiver sensitivity threshold is sufficient in most systems. RAD-80211-XD... modules provide a means for direct measurement of received signal strength using a DC voltmeter. See Section 6.2, “RSSI (Received Signal Strength Indicator)” for more information.

2.4 Antennas and Cabling

The single most important item affecting radio performance is the antenna system. Careful attention must be given to this part of an installation, or the performance of the entire system will be compromised. Quality high gain antennas should be used at all stations. The antennas should be specifically designed for use at the intended frequency of operation and with matching impedance (50 Ω).

Antennas are made by several manufacturers and fall into two categories – OMNI-directional and YAGI-directional (see Figure 2-1). An OMNI-directional antenna provides equal radiation and response in all directions and is therefore appropriate for use at master stations which must communicate with an array of remote stations scattered in various directions. OMNI antennas should also be used where clients will be mobile.

At remote fixed stations, a directional antenna, such as a YAGI is typically used. Directional antennas confine the transmission and reception of signals to a relatively narrow beam width, allowing greater communication range, and reducing the chances of interference from other users outside the pattern. It is necessary to aim these antennas in the desired direction of communication (i.e., at the master station).

The end of the antenna (farthest from support mast) should face the associated station. Final alignment of the antenna heading can be accomplished by orienting it for maximum received signal strength.

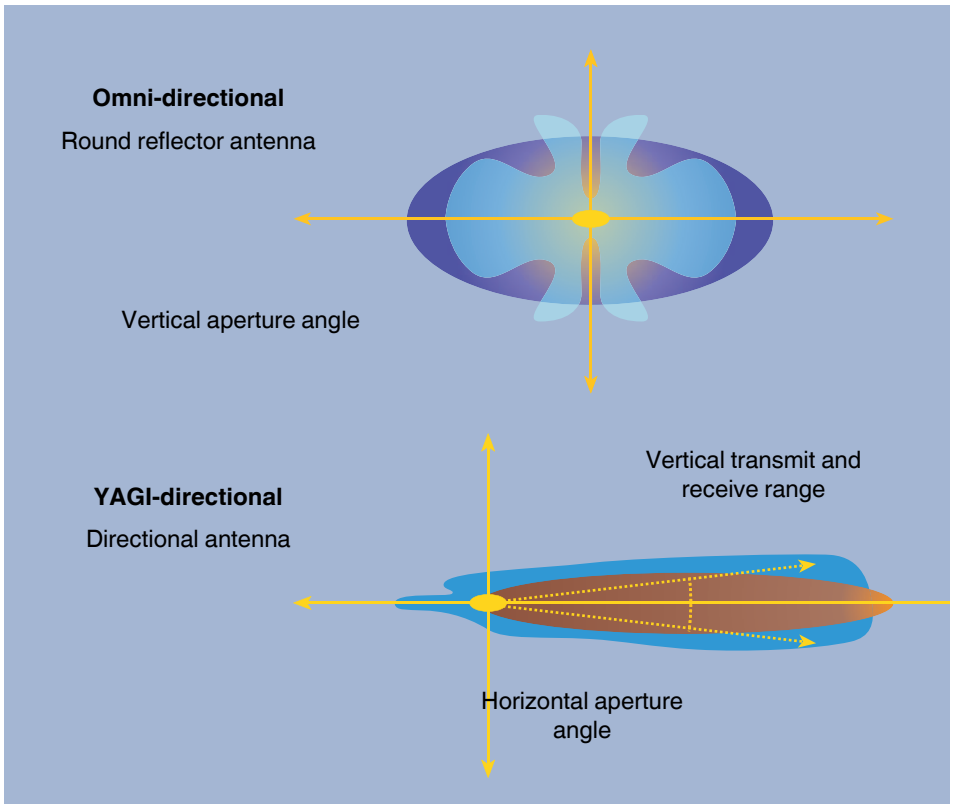


Figure 2-1 OMNI-directional and YAGI-directional Antenna Performance Characteristics

2.4.1 Coaxial Cable Considerations

The importance of using a low-loss antenna coaxial cable is often neglected during radio installation. Using the wrong cable can cause huge reductions in efficiency, and these losses cannot be recovered with any amount of antenna gain or transmitter power.

For every 3 dB of coaxial cable loss, half the transmitter power will be lost before reaching the antenna. The choice of coaxial cable to use depends on: 1) the length of cable required to reach the antenna, 2) the amount of signal loss that can be tolerated, and 3) cost considerations. For long-range transmission paths, where signal is likely to be weaker, a low-loss cable type is recommended. The higher operational frequencies of 802.11a (5 GHz) will be more prone to coaxial cable losses, and therefore more consideration should be given to low-loss cable.

For a short-range system, or one that requires only a short antenna coaxial cable, a less efficient cable may be acceptable and will cost far less than large diameter cable. Refer to Table 2-1 for values that allow judging the effectiveness of various cables at 2.4 GHz (802.11b and g) and 5 GHz (802.11a).

Table 2-1 Cable Types and Signal Loss (dB)

Cable Type	2.4 GHz Loss (dB/100 ft.)	5.2 GHz Loss (dB/100 ft.)	5.5 GHz Loss (dB/100 ft.)
RG-58	25.01	38.96	41.02
RG-213	12.51	20.56	21.79
LMR-240	12.76	19.37	20.31
LMR-400	6.68	10.27	10.79
LMR-500	5.41	8.41	8.85
LMR-600	4.37	6.87	7.24

2.5 Antenna Mounting Considerations

The antenna manufacturer's installation instructions must be strictly followed for proper operation of a directional or omnidirectional antenna. Using proper mounting hardware and bracket ensures a secure mounting arrangement with no pattern distortion or de-tuning of the antenna. The following recommendations apply to all antenna installations:

– Mount the antenna in the clear, as far away as possible from obstructions such as buildings, metal objects, dense foliage, etc. Choose a location that provides a clear path in the direction of the opposite antenna. If the antenna is co-located with another antenna (other than 2nd antenna connector on the same radio), try to get at least one foot vertical or one foot horizontal separation between the two.
– Polarization of the antenna is important. Most systems use a vertically polarized omnidirectional antenna at the master station. Therefore, the remote antennas must also be vertically polarized (elements perpendicular to the horizon). Cross-polarization between stations can cause a signal loss of 20 dB or more.
– When installed indoors, the radio must be grounded through the DIN rail for DIN-mount versions or using the ground lug on the wall-mount versions. A surge arrestor must be used on the antenna for outdoor installations.

2.6 Maintaining System Performance

Over time, any communications system requires a degree of preventative maintenance to ensure peak operating efficiency. Periodic checks of master and remote sites should be made to identify and correct potential problems before they become threats to system operation. The following areas should be given special attention:

2.6.1 Antennas and Coaxial Cable

Visually inspect the antenna and coaxial cable for physical damage, and make sure that the coaxial connections are tight and properly sealed against the weather. When using directional antennas, be sure that the antenna heading has not shifted since installation.

The SWR (Standing Wave Ratio) of the antenna system can be checked from time to time using a through-line wattmeter. Defects in the antenna system will frequently show up as reflected power on the meter. It is good practice to accept only a maximum reflected power of about 5%; this corresponds to an SWR of approximately 1.5:1. For any condition exceeding this value, search for and correct the cause—damaged antenna, defective or improperly installed connectors, water in the coaxial feedline, etc.

2.6.2 Cable Connections

All power, data, and ground connections should be secure and free of corrosion.

2.6.3 Power Supply

The voltage of the station power supply should be measured to verify that it is within the operating specifications for the radio. If possible, the radio should be keyed during this test to ensure maximum current draw from the supply. Batteries, if used, should be checked for charge level and signs of leakage or corrosion.

Section 3

This section informs you about
- Mounting the radios
- Power connections
- Ethernet and serial connections
- Antenna connections

Installation 3-3

3.1 Mounting the Radios 3-3
3.1.1 Mounting the RAD-80211-XD or RAD-80211-XD-BUS 3-3
3.1.2 Mounting the RAD-80211-XD-WM 3-6

3.2 Making Connections and Powering Up 3-8
3.2.1 Power Connections 3-8
3.2.2 Ethernet Connections 3-11
3.2.3 Serial Port Connections 3-11
3.2.4 Antenna Connections 3-13

3 Installation

3.1 Mounting the Radios

3.1.1 Mounting the RAD-80211-XD or RAD-80211-XD-BUS

Figure 3-1 shows a typical RAD-80211-XD or RAD-80211-XD-BUS radio installation using a Phoenix Contact power supply, end clamps and a DIN rail grounding block.

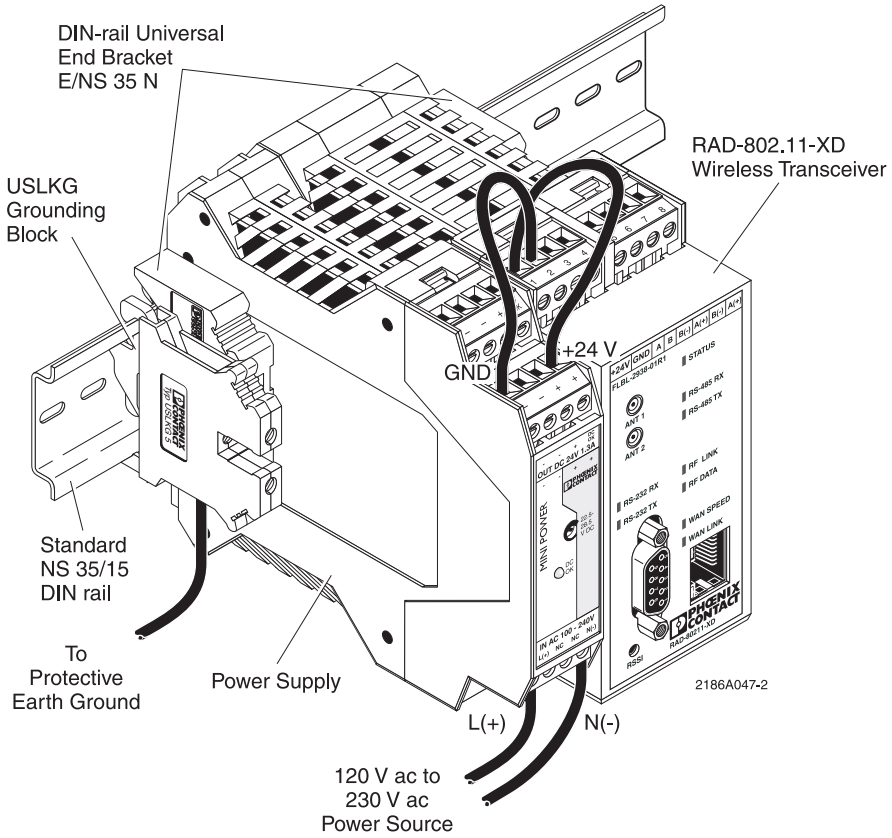


Figure 3-1 Installation showing a DIN rail power supply, end clamps and ground terminal block

When mounting the radio onto a standard 35 mm (1.378 in.) DIN rail, end clamps should be mounted on both sides of the module(s) to stop the modules from slipping on the DIN rail (see Figure 3-1).

Modules are installed from left to right on the mounting rail. Install modules to mounting rail as described in the following steps.

DANGER:

DO NOT CONNECT OR DISCONNECT EQUIPMENT UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS

When used within hazardous conditions (for Class I Division 2, Groups A, B, C and D), the RAD-80211-XD-WM product must be installed in an approved IP54 or NEMA 4X enclosure.

Installation is to be conducted by a license electrician as per the local installation/electrical codes.

WARNING:

Never install or remove a module while power is applied to any component on the rail. Before installing or removing a module, disconnect power to the entire station. Make sure work on the entire station is complete before switching power back on.

WARNING:

Do not connect or disconnect any connector while power is ON. This can cause arcing that could damage electronics or cause personal injury.

1. Attach the RAD-80211-XD or RAD-80211-XD-BUS module to the mounting rail by positioning the keyway at the top of the module onto the mounting rail. Then rotate the module inward until the DIN rail latch locks the module in place on the rail. Next, check that the module is fixed securely to the rail by lightly pulling outward on the module.

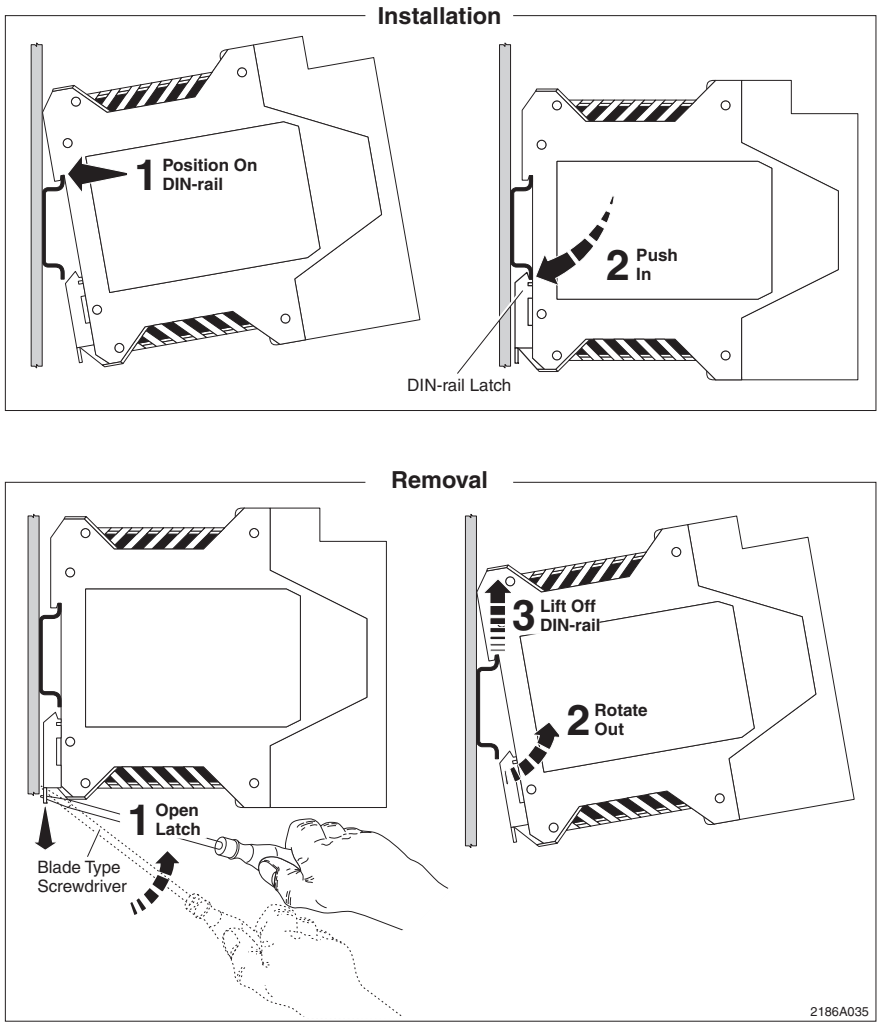


Figure 3-2 Installing and removing a module from the DIN rail

2. Continue attaching any other module(s) to the mounting rail as described in Step 1.

NOTE:
Phoenix Contact recommends the use of end clamps to prevent modules from moving back and forth on the mounting rail.

3. When all modules are installed, place an end clamp tight up against the left side of the left-most module on the mounting rail. Then place a second end clamp tight up against the right side of the right-most module on the mounting rail.

NOTE:

Grounding clips built into the RAD-80211-XD or RAD-80211-XD-BUS module make contact with the upper edge of the DIN rail during installation. This provides a ground path from the DIN rail to the module. To ensure proper shielding of the module(s) through the DIN rail, Phoenix Contact recommends connecting the DIN rail directly to a low impedance earth ground.

4. Connect the DIN rail to protective earth ground using a grounding terminal block (see Figure 3-1).

3.1.2 Mounting the RAD-80211-XD-WM

In areas where there is exposure to direct and continuous sunlight (UV) or rain, mounting under a protective cover is recommended.

DANGER:

Do not connect or disconnect equipment unless area is know to be non-hazardous.

When used within hazardous conditions (for Class I Division 2, Groups A, B, C and D), the RAD-80211-XD-WM product must be installed in an approved IP54 or NEMA 4X enclosure.

Installation is to be conducted by a license electrician as per the local installation/electrical codes.

WARNING:

Never install or remove a module while power is applied to any component on the rail. Before installing or removing a module, disconnect power to the entire station. Make sure work on the entire station is complete before switching power back on.

WARNING:

Do not connect or disconnect any connector while power is ON. This can cause arcing that could damage electronics or cause personal injury.

1. Mount the radio to a flat surface such as a wall (minimum 1/2-inch, drywall) or cabinet side using four No. 8-32 pan head screws at least 3/4-inch long. If mounting to drywall, use No. 8 screws with wall mounting anchors.

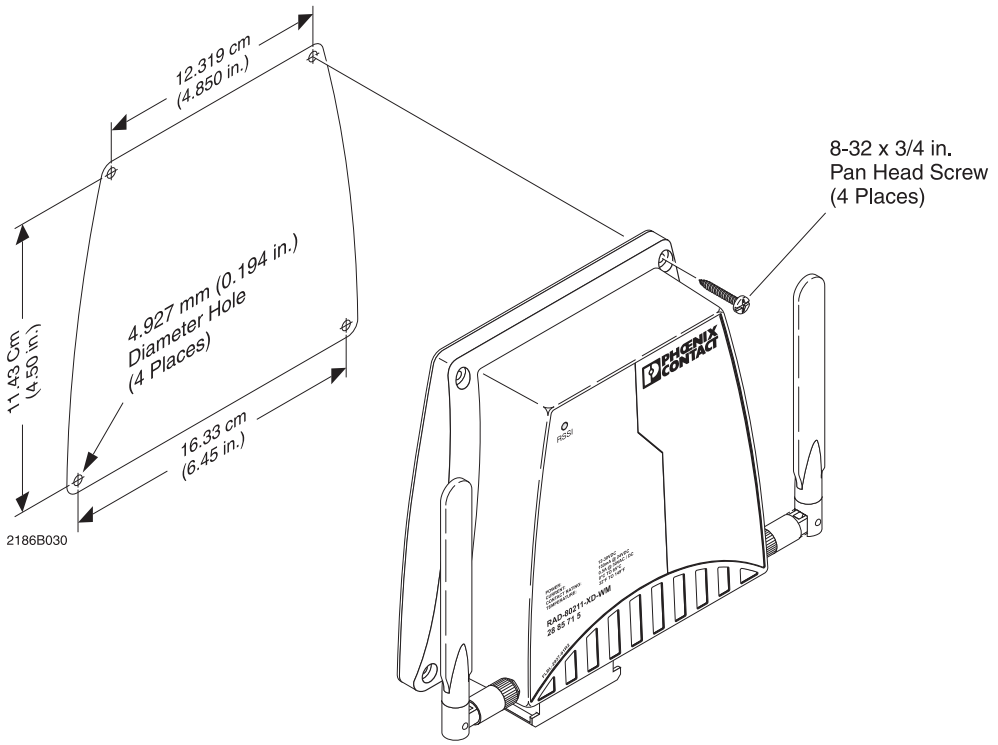


Figure 3-3 Typical installation of the RAD-80211-XD-WM radio

2. Connect the radio to protective earth ground using the ground lug located on the right side of the module.

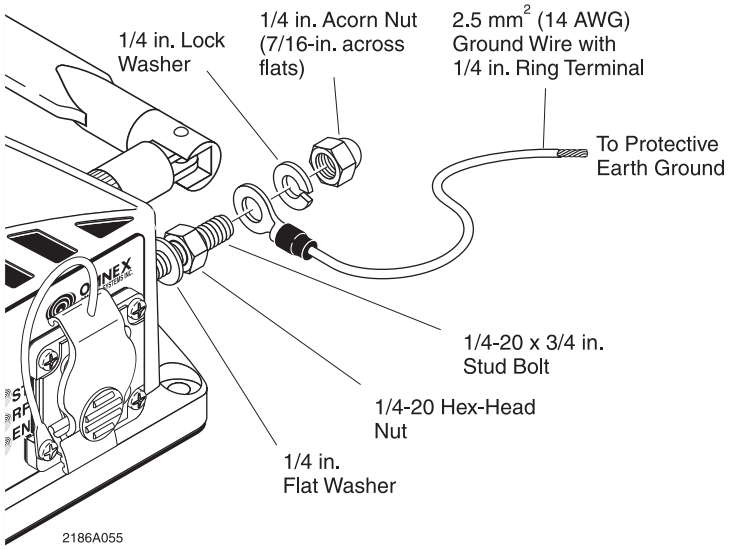


Figure 3-4 RAD-80211-XD-WM radio ground connection

3.2 Making Connections and Powering Up

3.2.1 Power Connections

External interconnecting cables are to be installed in accordance to NEC, ANSI/NFPA70 (for US applications) and Canadian Electrical Code, Part 1, CSA C22.1 (for Canadian applications) and in accordance to local country codes for all other countries.

RAD-80211-XD or RAD-80211-XD-BUS

Connect a regulated Class 2 DC power source to the transceiver. The supply voltage can range from 12 to 30 V DC with a nominal voltage of either 12 V DC or 24 V DC recommended. The power supply must be able to supply 150 mA of current at 24 V DC. Figure 3-5 shows an installation using a Phoenix Contact MINI power supply. Figure 3-6 provides wiring information for the RAD-80211-XD or the RAD-80211-XD-BUS.

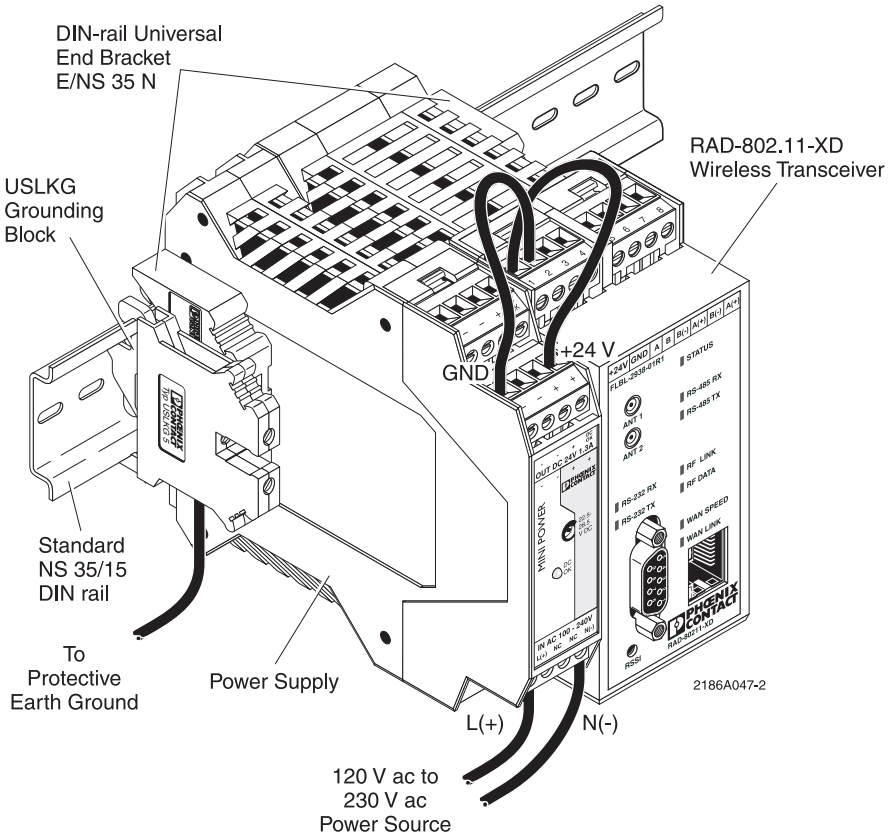


Figure 3-5 RAD-80211-XD or RAD-80211-XD-BUS power connections

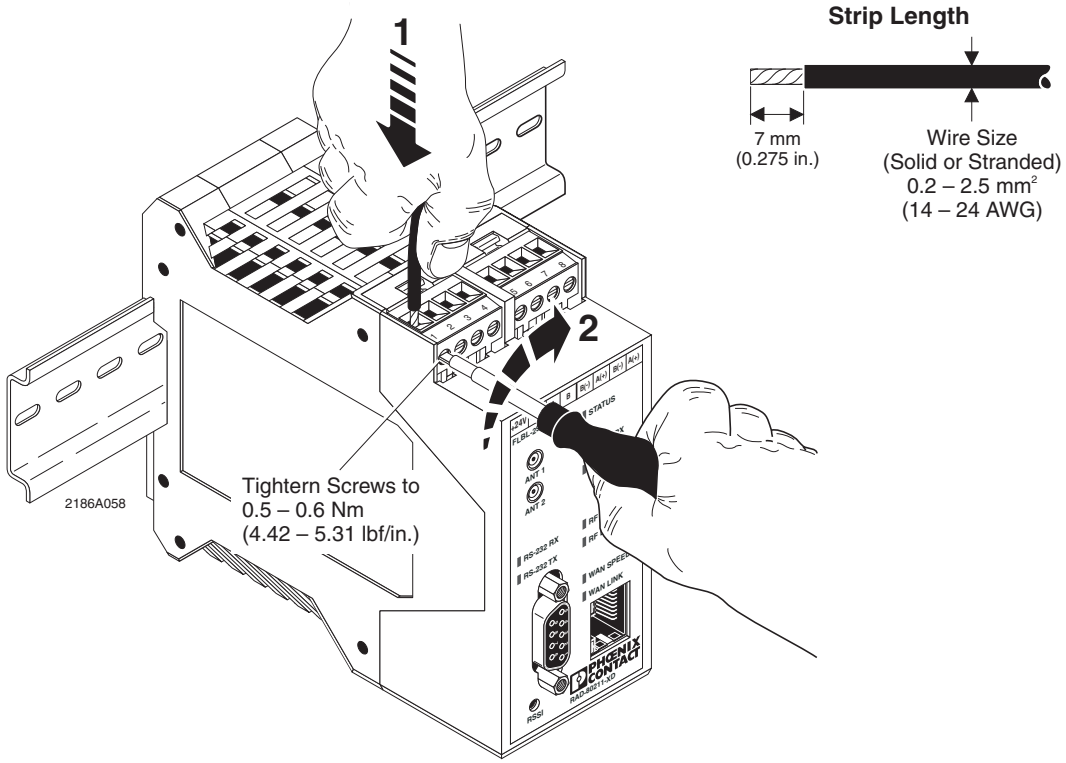


Figure 3-6 RAD-80211-XD or RAD-80211-XD-BUS transceiver wiring requirements

RAD-80211-XD-WM

The RAD-80211-XD-WM has two power options. The device may be powered from a Class 2 DC power supply ranging from 12 to 30 V DC or by a UL listed Power-over-Ethernet (PoE) using an 802.3af compliant power injector. Figure 3-7 and Figure 3-8 show how to make the connections. If redundancy is needed, the radio can be powered from both the DC source and using PoE. In this case the DC source is a backup power source in the event that primary power is lost. The DC source must be connected to the radio with an M12 connector. For example, the Phoenix Contact 1.5 m cable (Order No. 1668108) has an M12 connector on one end and flying leads on the other. Other cable lengths are available. Visit our web site at www.phoenixcontact.com.

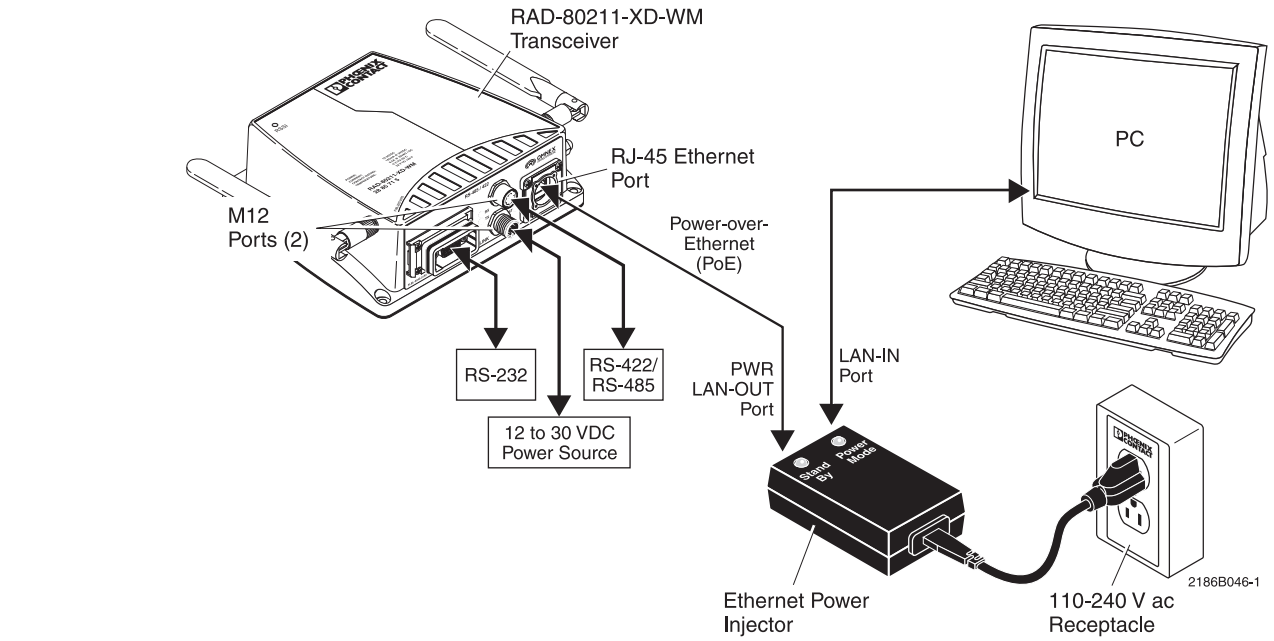


Figure 3-7 RAD-80211-XD-WM power connections

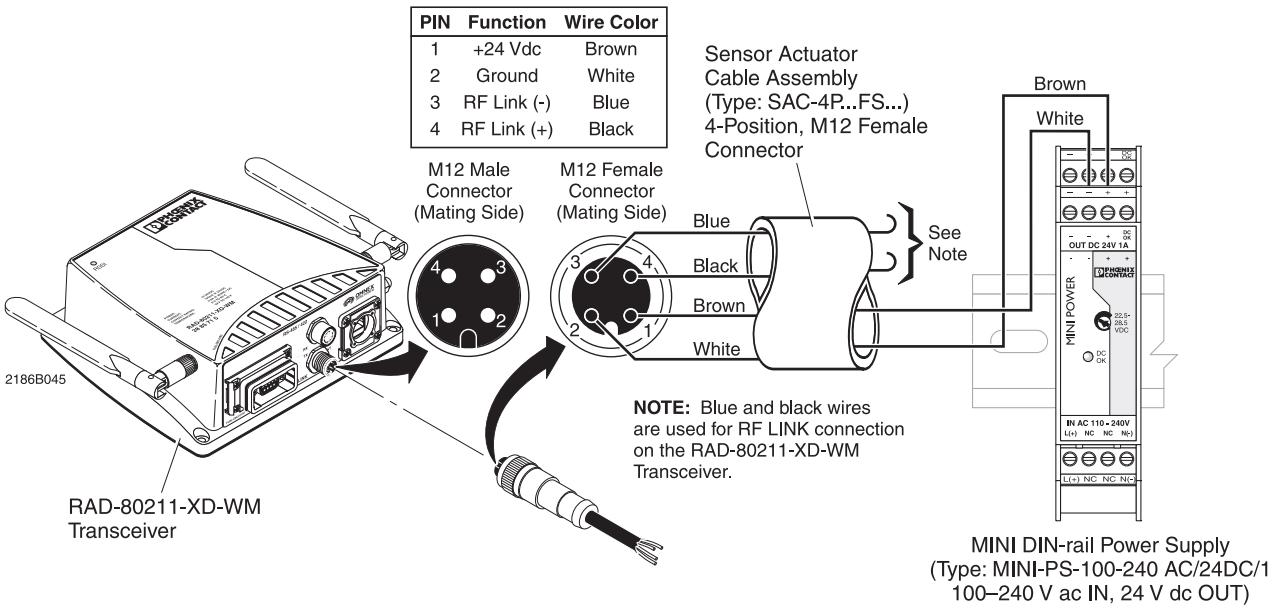


Figure 3-8 RAD-80211-XD-WM M12 cable connections

3.2.2 Ethernet Connections

Connect a CAT5 Ethernet cable between the port on the transceiver and the network adapter card on your computer. Use either a crossover (C/O) or 1:1 cable as the radio has autocross functionality. The cable should not exceed 100 m (329 ft.) in length.

3.2.3 Serial Port Connections

NOTE:

These ports are used for transferring data. Device configuration is done through the Ethernet port.

RS-232 Connections

When the correct RS-232 cable is used to connect the radio to the computer or PLC/industrial instrument, the TX LED on the radio will light. (This TX LED will also flash when data is passed.)

There are two types of serial port cables that both have DB-9 (9-pin D-sub) connectors (see Figure 3-9). One is called a straight-through 9-pin serial port cable and the other is called a null modem cable. On a straight-through cable, it is wired as just that – straight through, in other words, pin 1 is connected to pin 1, pin 2 to 2, etc.

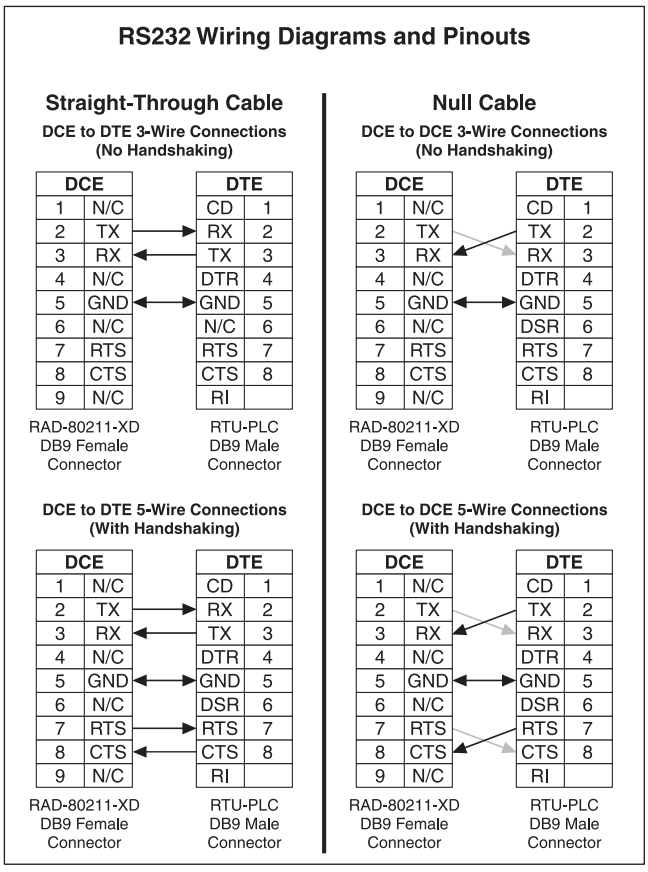


Figure 3-9 RS-232 wiring diagrams and pinouts

A null modem cable crosses over pins 2 and 3 (transmit and receive data) and also crosses over pins 7 and 8 (clear-to-send [CTS] and ready-to-send [RTS]. A null modem cable is designed to allow two devices to be connected together when they both function as data terminal equipment (DTE) or when they both function as data communications equipment (DCE). By swapping the pins, it connects inputs to outputs and vice versa for proper operation.

Equipment with serial ports can be designed as either DTE or DCE. This determines the functions of pins 2 & 3, and 7 & 8. For example, if pin 7 is an output on one end, then it will have to be an input on the other end. Computers are typically DTE devices while modems and radio modems are DCE. Programmable Logic Controllers (PLCs), flow computers and other industrial instruments could be either DCE or DTE.

To connect a DCE device to a DTE device, a straight-through cable is used. To connect two DCE devices together or to connect two DTE devices together, a null modem cable is required.

RS-422/485 Connections

The radio can also be connected to external devices using RS-485 or RS-422. Both 2-wire and 4-wire configurations are supported. Although the 4-wire configuration supports full duplex communications, the radio is only half duplex over the air.

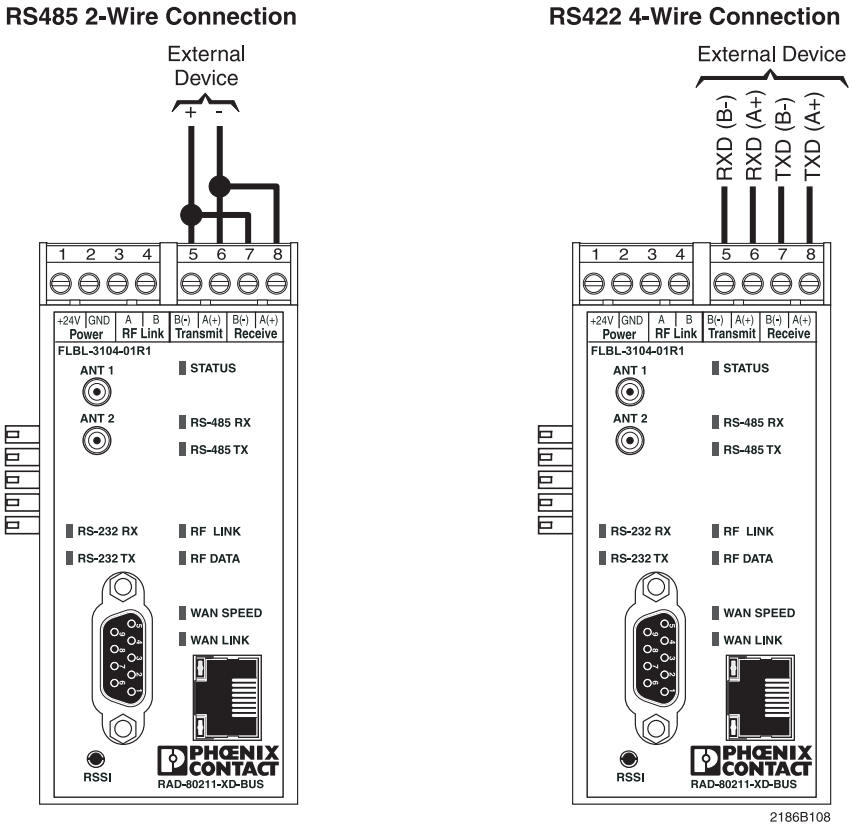


Figure 3-10 RS-422/485 2-wire and 4-wire connections

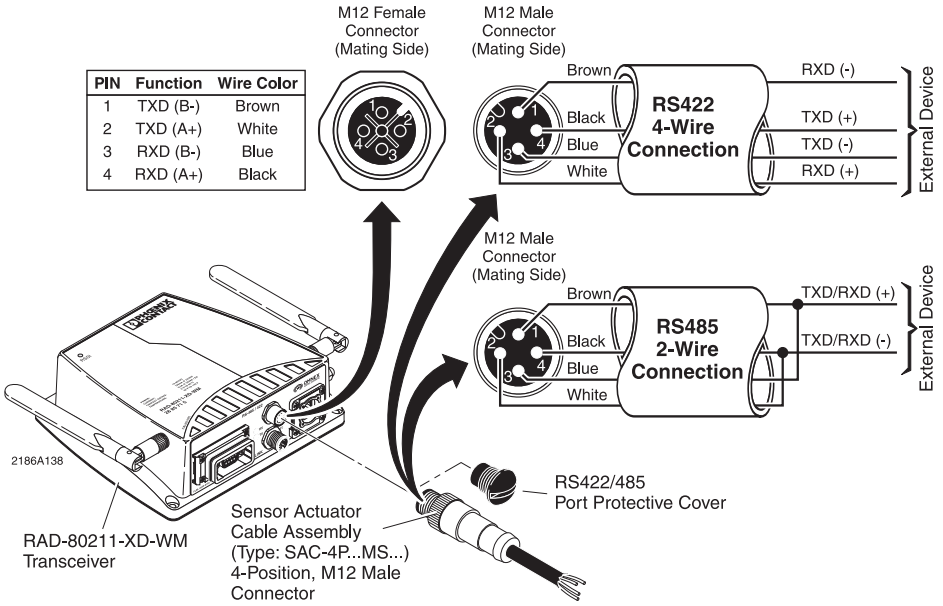


Figure 3-11 RAD-80211-XD-WM 2-wire and 4-wire connections

3.2.4 Antenna Connections

There are two antenna connectors on the transceiver (see Figure 3-12). A single antenna can be used or two antennas can be connected to provide antenna diversity (see “Additional Parts and Accessories” on page 8-6 for options).

Some sites may experience multipath problems. Multi-pathing is likely to be a greater problem when there is no line-of-sight and there are lots of metal structures in the path. Conductive metals reflect RF energy fairly efficiently and increase the possibility of a multipath condition. If there is clear line-of-sight, multipath is less likely to occur but can still be a problem. If using a single antenna, connect it to **ANT 1**.

NOTE:
If a single antenna is used, the protective cap must be installed on the **ANT 2** connector for the radio to meet the listed ESD specifications.

At least one antenna must be used. When using a single antenna, it must be connected to **ANT 1**.

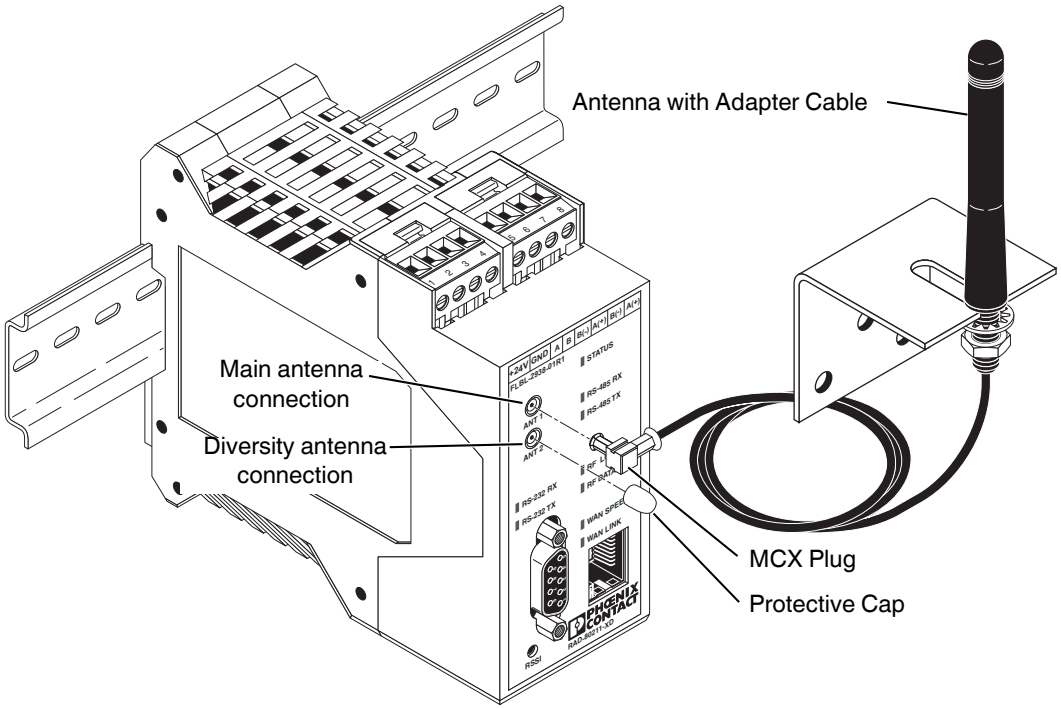


Figure 3-12 RAD-80211-XD or RAD-80211-XD-BUS Redundant Antenna Connections

To realize the benefits of antenna diversity, the antennas should be located at least 1.25 wavelengths apart. At 2.4 GHz, this distance is 15 cm (5.9 in.). At 5 GHz, this distance is 7 cm (2.8 in.). Antennas can be mounted farther apart, but most of the benefit is realized at 1.25 wavelengths.

NOTE:
Transceiver can use either the 2.4 GHz or 5 GHz ISM band. The antenna must be specific to the frequency. There are dual band antennas available if both frequency ranges are used. 802.11a uses the 5 GHz band whereas 802.11b and g use the 2.4 GHz band.

NOTE:

The maximum antenna (system) gain is restricted by the FCC (Federal Communications Commission) and ISC (Industry Science Canada).

In the 2.4 GHz band, the maximum EIRP (Effective Isotropically-Radiated Power) is limited to 4 W (36 dBm). The EIRP is calculated by adding the transmit power of the radio to the system gain of the antennas and coaxial cables measured in dBm.

Example:

– 1 W transmit power (30 dBm) +6 dBi system gain = 36 dBm
– 100 mW transmit power (20 dBm) +16 dBi system gain = 36 dBm

The 5 GHz band is divided into 2 portions of the spectrum with slightly different rules. In the UNII lower band: [5.25–5.35 GHz (channels 52, 56, 60, 64)], the maximum EIRP is 800 mW (29 dBm).

Example:

– 200 mW transmit power (23 dBm) +6 dBi system gain = 29 dBm
– 100 mW transmit power (20 dBm) +9 dBi system gain = 29 dBm

In the UNII upper band: [5.745–5.805 GHz (channels 149, 153, 157,161)], the maximum EIRP is 4 W (36 dBm).

– 800 mW transmit power (29 dBm) +7 dBi system gain = 36 dBm
– 100 mW transmit power (20 dBm) +16 dBi system gain = 36 dBm

Section 4

This section informs you about
– Configuring the PC to communicate with the radio

Programming the Radio 4-3

4.1 Configuring the PC to Communicate with the Radio 4-3
4.2 Logging Into the Radio 4-3
4.3 Viewing Device Information 4-4
4.4 General Device Information 4-5
4.5 Local Diagnostics 4-6
4.6 General Configuration 4-7
4.7 Operational Mode 4-8
4.8 LAN Configuration 4-9
4.9 SNMP Configuration 4-10
4.10 DHCP Server 4-11
4.11 Configuring the RAD-80211-XD... as an Access Point 4-12
4.11.1 General 4-12
4.11.2 Access Point Security 4-15
4.11.3 MAC Address Filtering 4-18
4.11.4 Rogue Access Point Detection 4-19
4.11.5 Advanced Settings 4-20
4.12 Client Configuration 4-21
4.12.1 General 4-21
4.12.2 Security 4-22
4.13 Bridge Configuration 4-25
4.13.1 General 4-25
4.13.2 Manual Bridging 4-25
4.13.3 Auto Bridging 4-26
4.13.4 Bridge Radio Settings 4-29
4.13.5 Bridge Security 4-30
4.14 I/O Ports 4-31
4.14.1 Ethernet Port 4-31
4.14.2 Serial Ports 4-32
4.14.3 PLC Interface (RAD-80211-XD-BUS only) 4-33
4.15 Passwords 4-34
4.16 Store and Retrieve Settings 4-35
4.17 Performance 4-36
4.18 Maintenance 4-36
4.18.1 Software Updates 4-37
4.19 Monitoring/Reports 4-38

4 Programming the Radio

4.1 Configuring the PC to Communicate with the Radio

NOTE:
The instructions below are for Windows XP operating system. Other versions of Windows will be similar but not identical. You may need to be logged in as an administrator to make these settings.

1. Go to the “Network Connections” dialog box, and then click “Local Area Connections” Right-click and select “Properties” from the context menu.
2. Highlight “Internet Protocol (TCP/IP),” and then click the “Properties” button.

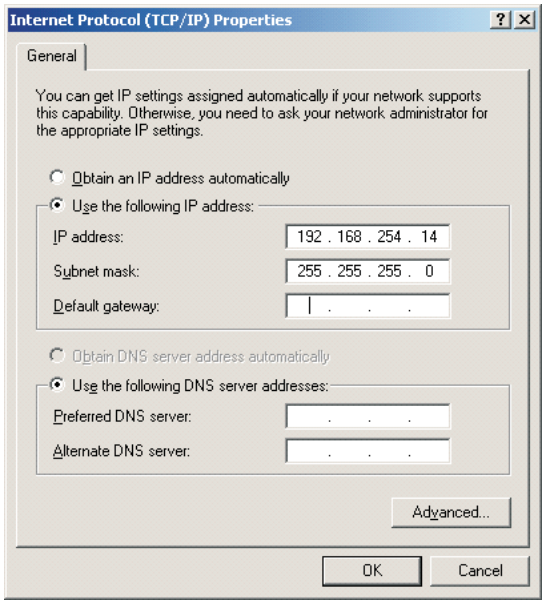

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 254 . 14
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 4-1 “Internet Protocol (TCP/IP) Properties” dialog box

3. Click the “Use the following IP address” radio button, and enter **192.168.254.xxx** (xxx can be between 2 and 253) in the “IP address:” field.
4. Enter **255.255.255.0** in the “Subnet mask:” field, and then click the “OK” button.

4.2 Logging Into the Radio

1. Apply power to the transceiver and run a browser program (such as Internet Explorer) on your computer. Wait approximately 10 seconds for the radio to boot up.
2. Enter the following IP address into the “Address” field of the browser:
   https://192.168.254.254

Enter the default case-sensitive credentials:

Username: Admin

Password: admin

3. Check the “Agree to the terms and conditions” box, and then click the “Sign In” button.

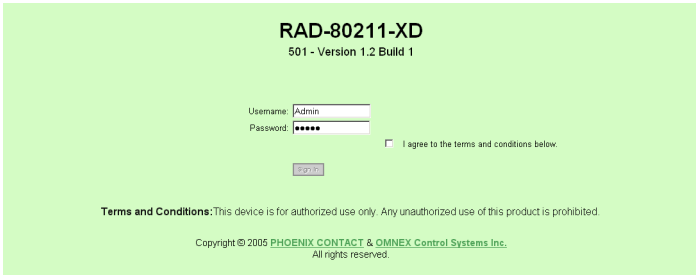

RAD-80211-XD
501 - Version 1.2 Build 1
Username: Admin
Password:
I agree to the terms and conditions below.
Terms and Conditions: This device is for authorized use only. Any unauthorized use of this product is prohibited.
Copyright © 2005 PHOENIX CONTACT & OMNEX Control Systems Inc.
All rights reserved.

Figure 4-2 “Sign In” screen

NOTE:

Powering multiple radios with factory default IP addresses will cause a network conflict, and incorrect parameters may be set in the radios. When programming radios for the first time, it is important to power on only one radio at a time, and change the IP address of each radio such that they are all unique (and different from the PC). Once each radio has a different IP address, they can be powered on together. The IP address of the radio can be changed under “Configuration… LAN… IP Configuration” and is described in “LAN Configuration” on page 4-9. The new IP address must be known in order to gain access to the radio in the future.

4.3 Viewing Device Information

After signing in, the home page shows the following basic information.

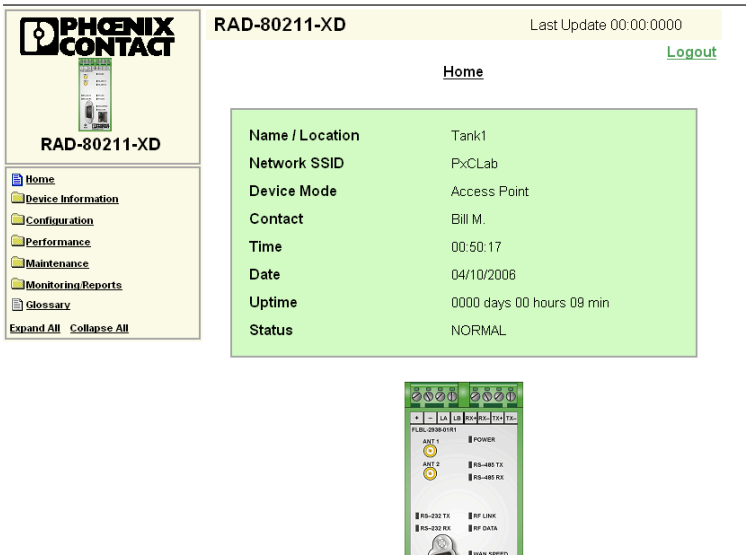


Figure 4-3 “Home” screen showing configuration data

The fields in this window are:

– **Name/Location** is a user-adjustable field. Information on where this radio was installed or the site name is shown here. The factory default is a blank field.
– **Network SSID** is the System Security ID. The Network SSID only appears when the radio is configured as an access point. The factory default is “default”.
– **Device Mode** shows if the device is programmed as an access point, client or a bridge.
– **Contact** is the name of the individual responsible for the operation of this radio.
– **Time** is the time of the radio’s internal clock.
– **Date** is the date of the radio’s internal clock.
– **Uptime** shows how long the radio has been operating.
– **Status** tells if the radio is operating normally, or if it has encountered any internal or configuration errors.

4.4 General Device Information

Click on “Device Information… General” in the left navigation column to view the current network configuration and device version of the transceiver.

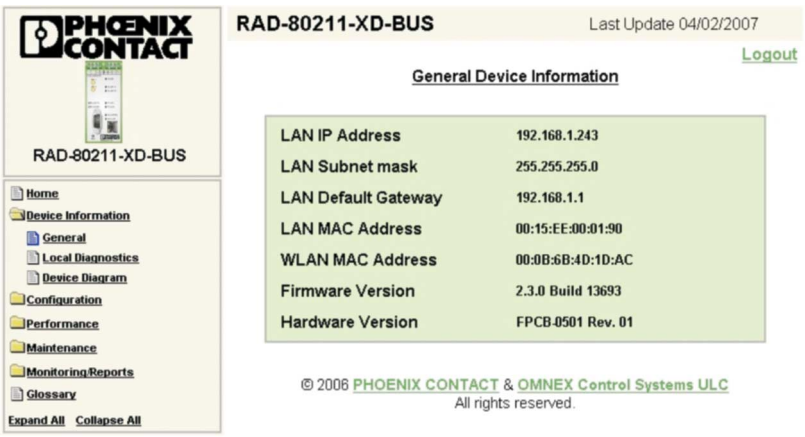


Figure 4-4 “General Device Information” screen

The fields in this window are:

– **LAN IP Address** is the logical address of a network adapter. The IP address uniquely identifies this radio on the network.
– **LAN Subnet Mask** is a bit mask used to tell how much of an IP address identifies the subnetwork the host is on, and how much identifies the host.
– **LAN Default Gateway** is a node on the network that serves as an access point to a different network (possibly the Internet).
– **LAN MAC Address** (Media Access Control address, MAC address) is a unique identifier attached to most forms of networking equipment. It is the physical address of the hardwired Ethernet port that is permanently assigned by the manufacturer.
– **WLAN MAC Address** is the address for the wireless card. Note that there are separate MAC addresses for the wireless card and the physical Ethernet port.
– **Serial Number** is the manufacturer’s serial number of the radio.

– **Firmware Version** identifies the version of software loaded into the radio. This is important in the event upgrades become available.
– **Hardware Version** identifies the version and revision level of the circuit boards.

4.5 Local Diagnostics

Click on “Device Information… Local Diagnostics” in the left navigation column to view the diagnostic information for the connected radio.

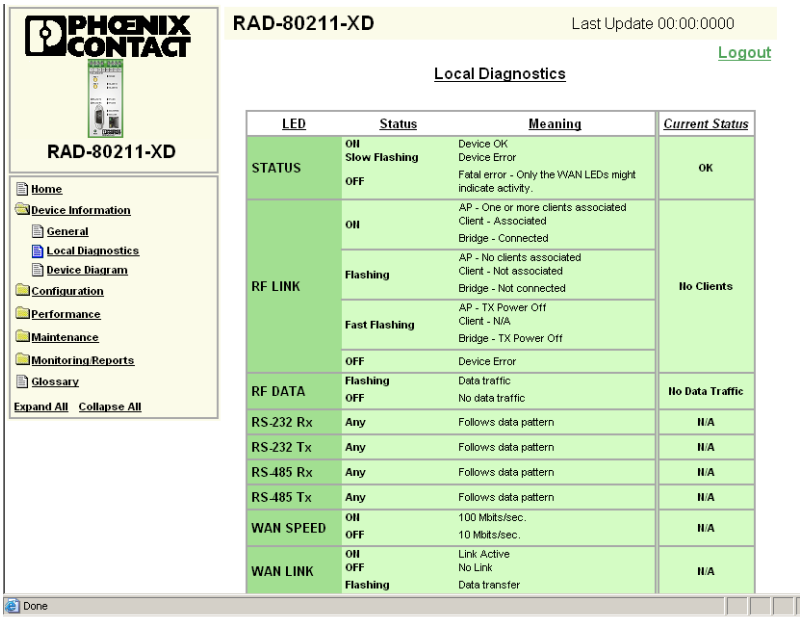


Figure 4-5 “Local Diagnostics” screen

This screen shows the current status and function of each LED on the radio and is useful for diagnostic purposes. For more information on the status LEDs, see Section 5, “XD-BUS Configuration for I/O Modules (RAD-80211-XD-BUS only)”.

4.6 General Configuration

To begin configuring the radio for a specific application, click on “Configuration… General” in the left navigation column.

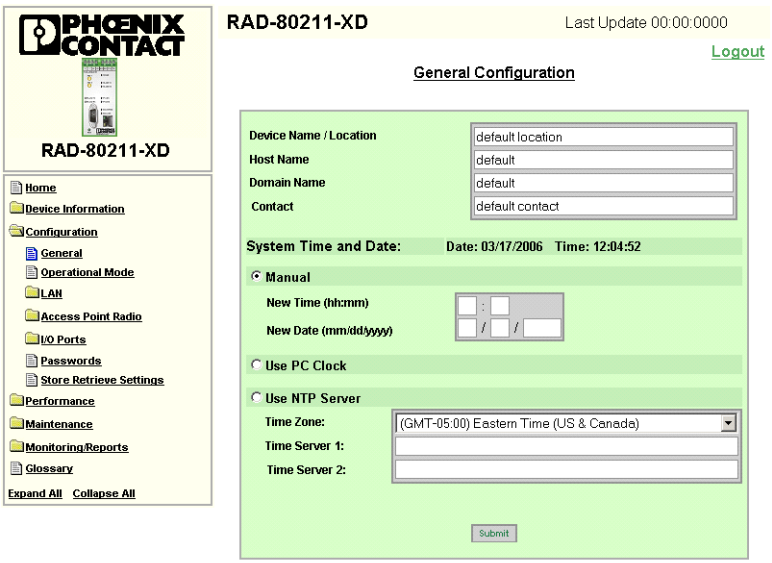


Figure 4-6 “General Configuration” screen

The buttons and fields in this window are:

– **Device/Location** and **Host Name** permits entry of text data to name this radio or location. This is only used to help the network administrator identify this radio from others.
– **Domain Name** permits entry of the domain name of this radio. This information is text only, and has no impact on network operation.
– **Contact** permits entry of the name of the network administrator or individual responsible for this equipment.
– **System Time and Date** provides three methods for the radio to determine the time and date: manually set the time and date, sync the radio’s clock from the PC’s internal clock or use an NTP Server. The radio uses a super capacitor to allow it to retain the date and time in the event of a power outage.

If deciding to use an NTP server, there must either be one connected to the LAN/WAN, or the radio must be connected to the Internet. Enter the server address. One example is the University of Houston’s NTP server, which requires the address be entered as follows:

tick.uh.edu

Click the “Submit” button to write the configuration to the radio.

NOTE:

If no functions are performed for 10 minutes, the program will exit and the parameters will need to be re-entered. It is generally good practice to select the “Submit” button after all parameters have been adjusted on each screen.

4.7 Operational Mode

Click on “Configuration… Operational Mode” in the left navigation column to configure the radio to function as an access point, client or bridge.

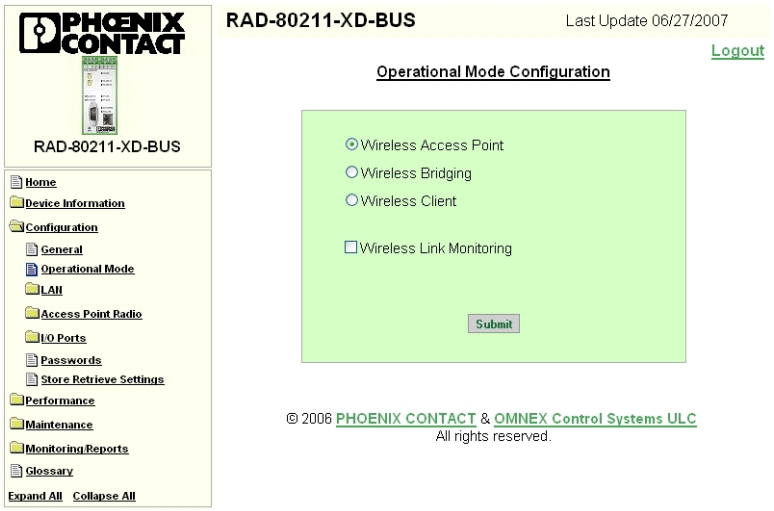


Figure 4-7 “Operational Mode Configuration” screen

NOTE:
When the “Wireless Link Monitoring” check box is not selected, the MAC addresses of other company’s radios and …80211… radios are displayed in the various status report web pages. Enabling “Wireless Link Monitoring” displays both the IP and MAC address of Phoenix Contact wireless devices only (if equipped with firmware 2.4 and higher).

When the operational mode is changed, the radio reboots. It may take several minutes for the radio boot process to complete.

4.8 LAN Configuration

NOTE:
This configuration step can be skipped if the radio is functioning as a repeater.

Click on “Configuration…LAN… IP Configuration” in the left navigation column to show the Local Area Network (LAN) configuration parameters.

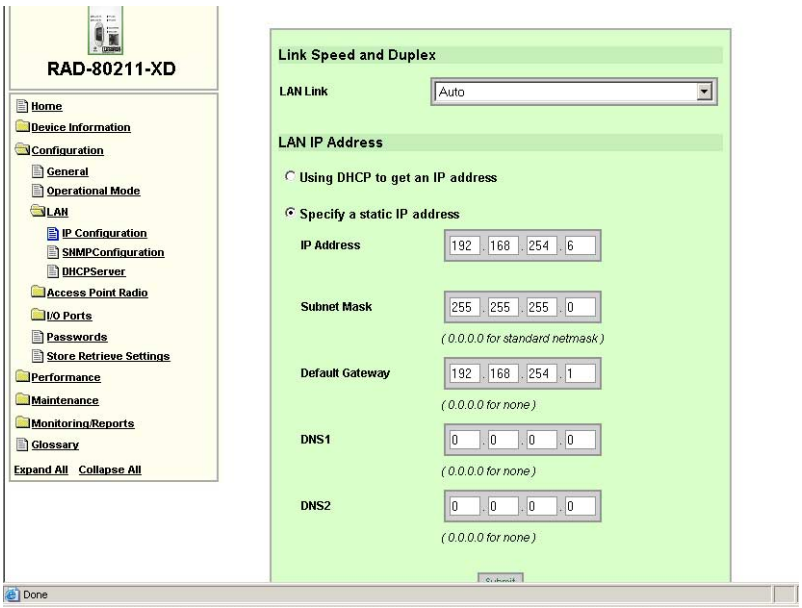


Figure 4-8 RAD-80211-XD LAN Configuration

The buttons and fields in this window are:

– **LAN Link Speed and Duplex** determines the speed the radio communicates with the wired LAN (if applicable). Leave the setting at AUTO to have the radio determine the speed. The radio and the device it is hardwired to must be set the same.
– **LAN IP Address** selects the method your network uses to obtain IP addresses. If using static IP addresses, enter the IP address assigned to the radio. Each device on the network must have a different IP address.

If a DHCP server is on the network and will assign IP addresses to the RAD-80211-XD... modules, click the “Use DHCP To Get IP Address” radio button.

NOTE:
If the IP address is changed from the factory default, you will need to know this in order to log back into the radio for future configuration changes. If DHCP addressing is used, additional software may be necessary to determine the IP address based on the MAC address of the radio.

Enter a “Subnet Mask” and “Default Gateway,” if desired.

To access the Internet though this device, enter the IP address of the domain name server(s) in the “DNS 1” and “DNS 2” fields.

4.9 SNMP Configuration

The Simple Network Management Protocol (SNMP) forms part of the Internet protocol that is used for monitoring the health and welfare of network equipment like routers and computers. To configure SNMP, click on “Configuration… LAN… SNMP Configuration” in the left navigation column.

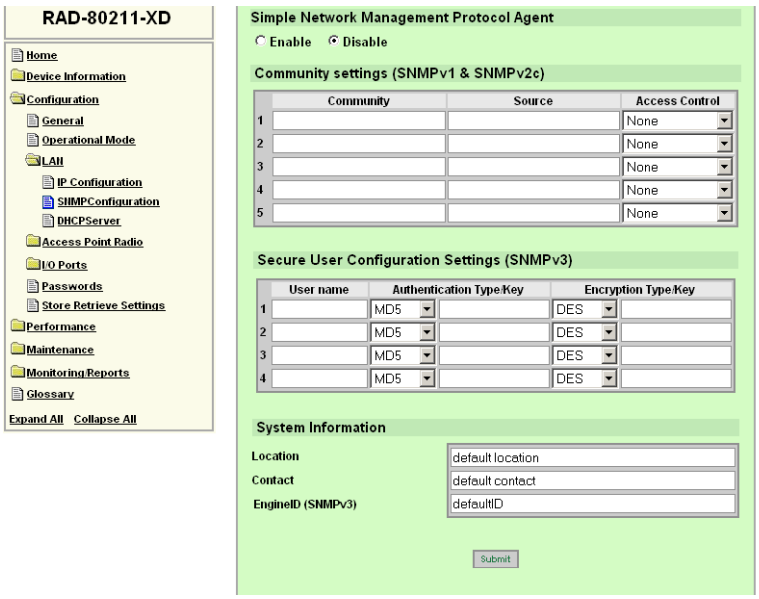


Figure 4-9 “LAN - SNMP Configuration” screen

The RAD-80211-XD... radios generate SNMP traps when one of the following events occurs:

– Cold start – when the device powers up.
– Warm start – generated when the user invokes the Reboot option in the web interface.
– Link up – generated whenever the client configuration is changed after the wireless client interface is restarted.
– Link down – generated whenever the client configuration is changed before the wireless client interface is restarted.
– Authentication failure – generated when the user fails to authenticate via the web interface.

The buttons and fields in this window are:

– **Enable** use this button to enable and enter parameters in the “Community Settings” and/or “Secure User Configuration Settings” fields.
– **Community Settings** is a string of up to 30 characters. The community name acts as a password and is used to authenticate messages sent between an SNMP client and a device containing an SNMP server. The community name is sent in every packet between the client and the server.
– **Source** is an IP Access List that identifies the IP addresses of SNMP managers permitted to use a given SNMP community. An example of the network address format is 192.168.42.182/24. The subnet mask of the network is typically annotated in written form as a “slash prefix” that trails the network number.
– **Access Control** determines if the community has read/write access.

- **Secure User Configuration Settings** is the configuration for SNMP version 3.
- **User Name** is a string of up to 30 characters.
- **Authentication Type** indicates the algorithm used for authentication; it can be either MD5 or SHA, the latter one being the better algorithm.
- **Authentication Key** is a string of characters used for authentication. Maximum length is 42 characters.
- **Encryption Type** defines the encryption algorithm used by the SNMP protocol, and it can be either DES or AES. AES is the strongest encryption algorithm.
- **Encryption Key** is a string of up to 32 characters.
- **System Information**:
  - **Location** is the device's physical location, a string of up to 64 characters.
  - **Contact** is the person who manages the device, a string of up to 64 characters.
  - **Engine ID** uniquely identifies the agent in the device. Each SNMPv3 agent has an engine ID. The engine ID may be set by the network administrator and is unique to that internal network. It is a string of up to 48 characters.

4.10 DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server provides configuration parameters to the devices on the network. This information includes IP addresses and a network mask. There can only be one DHCP server on the network. Only an access point can be configured as a DHCP server. The IP addresses are the unique identifier that each piece of equipment on the network must have.

To configure the radio to function as a DHCP server, click on "Configuration… LAN… DHCP Server" in the left navigation column.

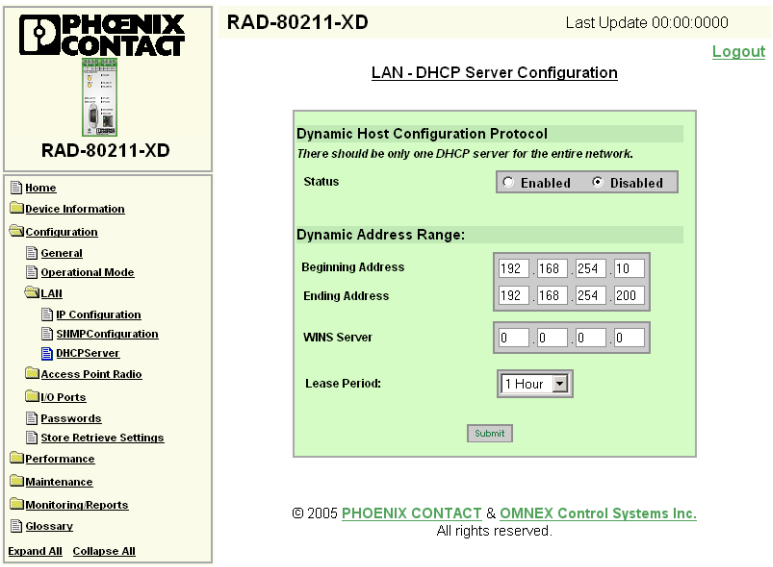


Figure 4-10 RAD-80211-XD DHCP Configuration

The buttons and fields in this window are:

Status lets you select “Enabled” to turn ON the DHCP server.

Dynamic Address Range provides the beginning and ending available IP addresses that devices on the network can use. Any value within this range may be assigned to nodes on the network.

WINS Server sets the IP address of the Windows Internet Naming Service.

Leased Period specifies the lease period of the assigned DHCP address.

4.11 Configuring the RAD-80211-XD... as an Access Point

4.11.1 General

To configure the radio as an access point (after selecting “Configuration… General” and then “Access Point”), click on “Configuration… Access Point… General” in the left navigation column.

This screen is only available after configuring the radio as a Wireless Access Point (see “Operational Mode” on page 4-8).

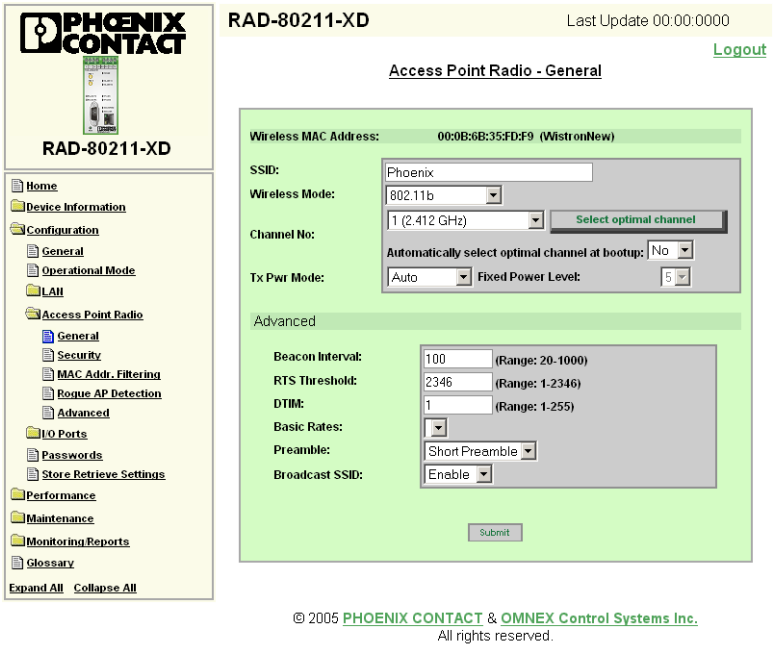


Figure 4-11 “Access Point Configuration” screen

The buttons and fields in this window are:

– **SSID** specifies an SSID for the wireless network. The factory default SSID is “default”. In order for a client to connect to the access point, it must have the same SSID.

– **Wireless Mode** specifies a desired wireless mode. Select 802.11a when using only 802.11a clients in the 5 GHz band. This will provide a stronger wireless network if there are existing 802.11b/g networks in the area, or there are other nearby sources of interference in the 2.4 GHz band. 802.11a and g have higher throughput than 802.11b (54 Mbps compared to 11 Mbps).
– **Channel Number** specifies one of 11 channels to use in the 2.4 GHz band (802.11b/g) (see Figure 4-12). All of the channels overlap with the exception of 1, 6 and 11. Separate wireless networks should use different channels, preferably non-overlapping. All radios in a wireless network must use the same channel.

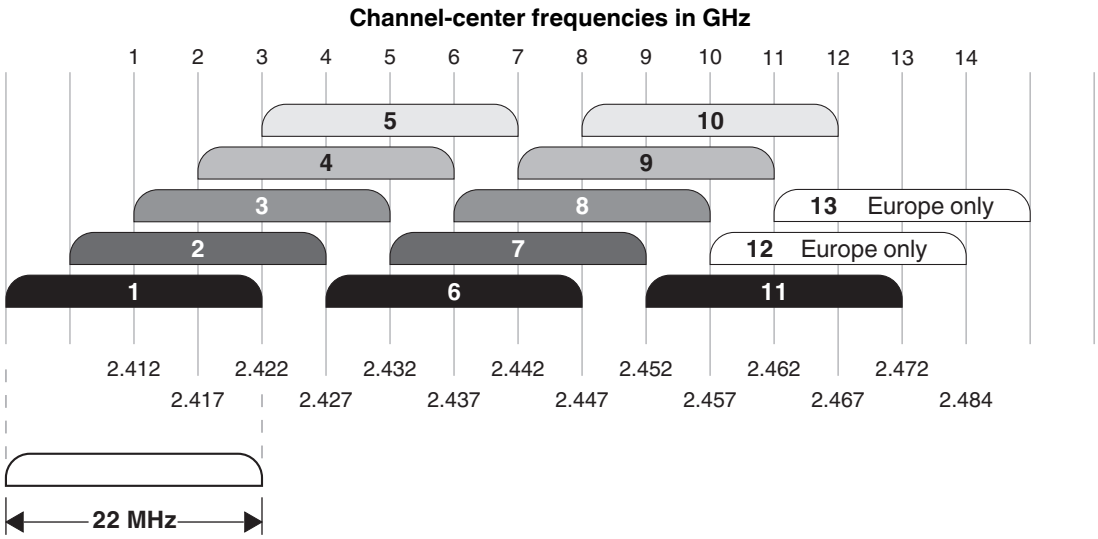


Figure 4-12 Channel-center frequencies (GHz) for 802.11b/g

If 802.11a is selected, there are 13 non-overlapping channels to choose from: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161 (see Figure 4-13).

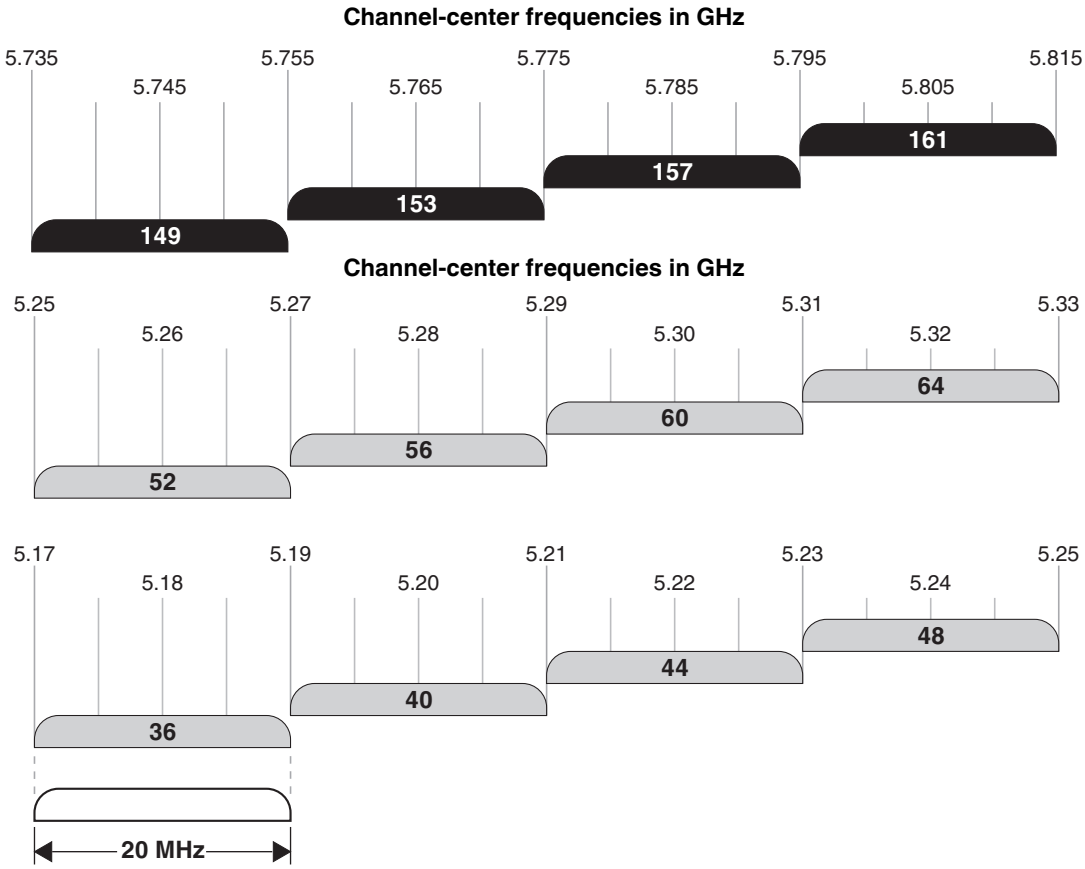


Figure 4-13 Channel-center frequencies (GHz) for 802.11a

If uncertain about which channel to use, click the “Select the Optimal Channel” (in 802.11b or g modes only) to let the radio scan for the channel with the least amount of interference. Clients will automatically determine which channel the access point is operating on.

– **Tx (Transmit) Power Mode** defines either fixed transmit power or lets the radio determine how much power is necessary to communicate with clients. In “Auto” mode, the access point will monitor the signal strength from the client. If it begins to get weak, it will automatically boost the transmit power. This works well with mobile clients. Note that the client must have the same amount of transmit power/antenna gain in order to send information back to the access point. The range will be dictated by the radio with the least amount of transmit power.
– **Advanced Settings** provides additional settings. Use factory defaults if you are unsure of these parameters.
– **Beacon Interval** is the time interval in milliseconds in which the 802.11 beacon is transmitted by the access point. A higher setting decreases time for a client to connect but decreases bandwidth utilized.

– **RTS Threshold** is the number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
– The **DTIM** field sets the number of beacon intervals between DTIM messages. Embedded within the beacon, a DTIM message informs a radio that a message is buffered for a client in power save mode.
– **Basic Rates** defines the basic rates used and reported by the access point. The highest rate specified is the rate that the access point uses when transmitting broadcast/multicast and management frames. The RF range of the units will increase as the data rate decreases. It may be desirable to select a lower data rate to maximize range.
– **Preamble** defines the preamble used to synchronize and set up bit timing on receiving radios. Older 802.11b systems require long preambles. Newer 802.11a/b/g systems can use both short or long. Short preamble is more efficient for data throughput. All radios must be set the same.
– The **"Broadcast SSID"** drop-down menu can be set to enable or disable. When enabled, the SSID is visible to other radios on the network. When disabled, the access point radio hides the SSID in outgoing beacon frames, and other radios cannot obtain the SSID through passive scanning. Also, when disabled, the access point doesn't send probe responses to probe requests from clients with unspecified SSIDs.

When the configuration parameters are changed, communication with other radios will be interrupted for 2 to 4 seconds.

4.11.2 Access Point Security

To enable and configure security, click on "Configuration… Access Point… Security" in the left navigation column.

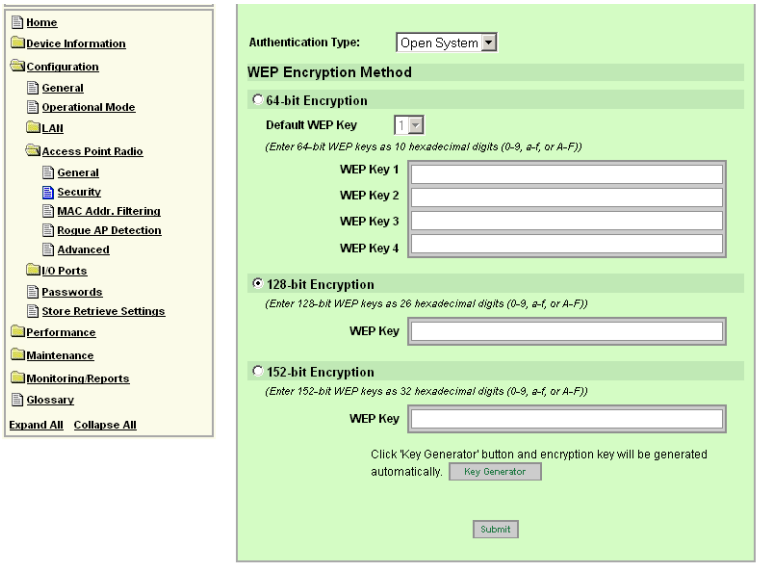


Figure 4-14 Access Point Radio - Security" screen showing Static WEP options

From the “Security Method:” drop-down menu, select the type of security desired: Static WEP, IEEE 802.11i and WPA™, or MAC Address Filtering.

Static WEP

The buttons and fields in this window are:

– The **Authentication Type** drop-down menu provides selection of “open,” “shared” or “open/shared” (clients may employ either). “Shared” provides slightly higher security; however, all clients must also have shared enabled as well. See “Access Point and Client Encryption” on page 1-12 for more information.

– **WEP Encryption Method** selects one of three sizes of keys that can be used by WEP. Larger keys will provide a higher level of security. Select the size of key and enter a key using only hexadecimal characters and no spaces (0-9 and A-F). Make a note of this key as it must be entered in all of the client radios. Click the “Key Generator” button to have the program automatically generate a key. Copy the key into other radios this unit must communicate with.

– **WEP Keys 1-4 (64-bit encryption)** selects one of four possible keys that can be used with 64-bit encryption. This serves the purpose of allowing periodic rotation of the WEP key by the operator. Simply select which key is desired. The same key must be chosen in the access point and all clients for successful operation. Only one key will be used at a time. Copy the key into other radios this unit must communicate with.

IEEE 802.11i and WPA Security

WPA and 80211i (WPA2™) selects the method of security from either WPA, 802.11i (WPA2) or both. WPA2 is more advanced and secure than WPA. WPA implements only a subset of the encryption algorithms used in WPA2. By implementing both WPA and WPA2,

wireless clients using either type of encryption will be allowed to connect and communicate. This is useful when older devices incapable of WPA2-encryption are used in conjunction with WPA2-enabled client devices.

Figure 4-15 “Access Point Radio - Security” screen showing 802.11i and WPA options

The buttons and fields in this window are:

– **Pre-Shared Key or 802.1x** specifies that you do not have an authentication server in your network. This is recommended for personal and small office networks that do not have an authentication (RADIUS) server. Each user must enter a passphrase with a minimum of eight (8) characters to access the network. Copy the passphrase into other radios this unit must communicate with.

The weak passphrases users typically employ create a major vulnerability to password cracking attacks. A longer passphrase is much stronger than a short one. A good method of creating a secure passphrase is to utilize an easy to remember sentence rather than just a word. Create the passphrase using the first letter of each word in the sentence. An example sentence would be:

– The Quick Brown Fox Jumped Over The Lazy Dog.
– The passphrase would be: TQBFJOTLD

NOTE:

Passphrases should be changed whenever an individual with access is no longer authorized to use the network or when a device configured to use the network is lost or compromised.

For maximum security, 802.11i requires the use of an authentication (RADIUS) server.

– **Pairwise Key** provides TKIP (Temporal Key Integrity Protocol) and AES-CCMP selections. For additional information, refer to “WPA with TKIP/AES-CCMP Encryption” on page 1-12. If all clients will use WPA-TKIP, click the “TKIP” check box. If all clients can use WPA-AES, click the “AES-CCMP” check box. Both may be enabled if a mix of clients with TKIP and AES-CCMP exists.
– **Radius Server** is an option for business applications that have installed RADIUS servers, Click the “802.1x” check box and enter the “Radius Server IP address” and a “Shared Secret” in the appropriate fields. Use of a RADIUS server for key management and authentication requires installation of a separate certification system, and each client must have been issued an authentication certificate.

  The “Group Encryption Key Lifetime” is for this purpose. This is the handshaking protocol between the access point and client radios in WPA, and is transparent to the user.

4.11.3 MAC Address Filtering

To enable MAC Address Filtering, click on “Configuration… Access Point… MAC Address Filtering” in the left navigation column.

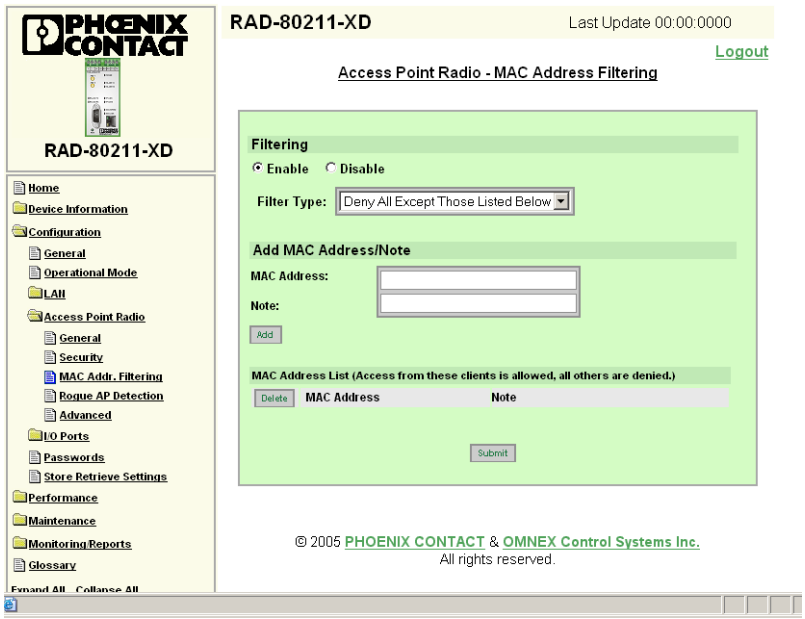


Figure 4-16 “Access Point Radio - MAC Address Filtering” screen

To use the feature, select the “Enable” radio button. Then select whether to exclude certain MAC addresses or include only certain MAC addresses. Enter MAC addresses accordingly; optionally include some text describing the device, and then click the “Add” button. To delete a MAC address, click the “Delete” button.

4.11.4 Rogue Access Point Detection

When Rogue AP Detection is enabled, it informs the administrator if a rogue access point is set up and attempting to log into the network. To enable, click on “Configuration… Access Point… Rogue AP Detection” in the left navigation column.

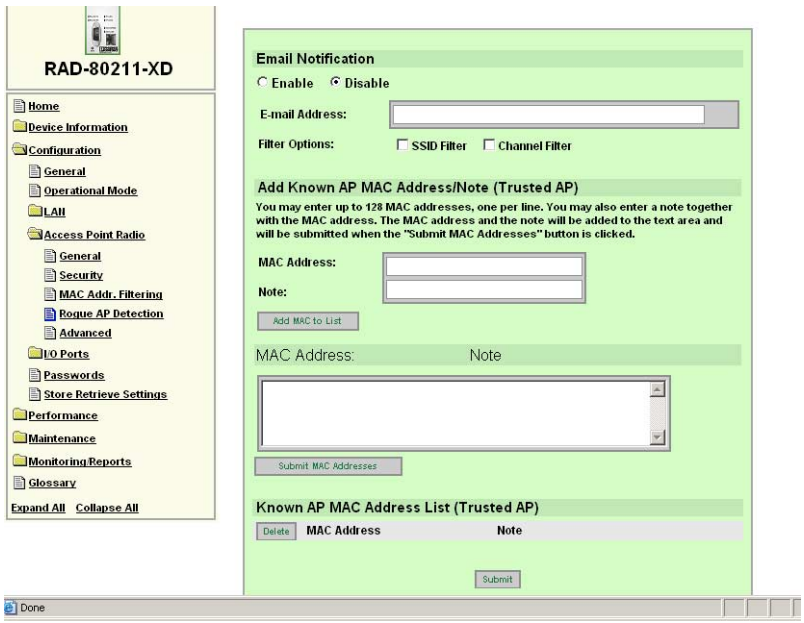


Figure 4-17 “Access Point Radio - Rogue AP Detection” screen

The buttons and fields in this window are:

– **E-mail Notification** specifies that an e-mail message is sent upon detection of a rogue access point. Click the “Enable” button and enter the receiving e-mail address in the “E-mail Address” field. To be alerted if the rogue access point has a different SSID, click the “SSID Filter” check box. To be alerted if a radio is operating on a different channel, click the “Channel Filter” check box.

– **Known AP MAC Address List (Trusted AP)** allows known or trusted access point MAC addresses to be explicitly set. There may be a number of known access points that are part of the network. Enter the MAC addresses of these known access points to prevent false alerts. Additionally, text may be entered in the notes field describing each MAC address.

4.11.5 Advanced Settings

Advanced options, such as load balancing and restricting inter-client communications, can be configured under Advanced Settings. To access this screen, click on “Configuration… Access Point… Advanced” in the left navigation column.

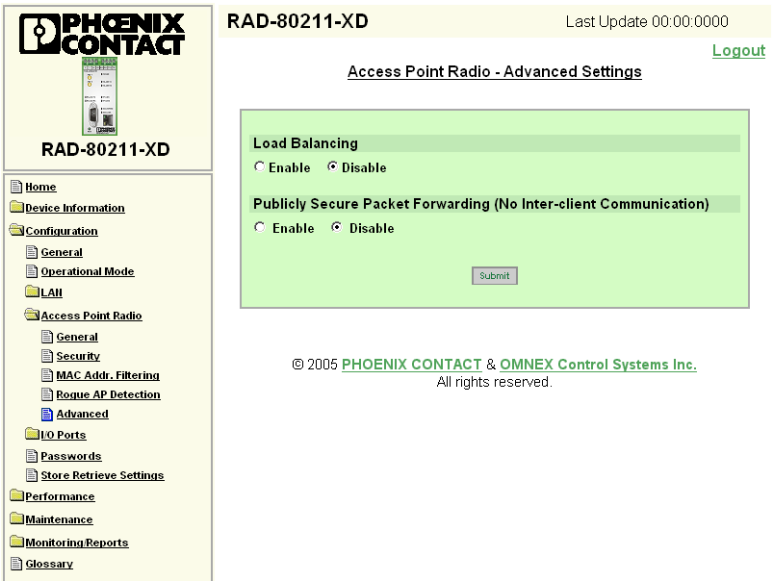


Figure 4-18 “Access Point Radio - Advanced Settings” screen

The buttons in this window are:

– **Load Balancing** forces access points to share clients evenly. If there are multiple clients within range of more than one access point, 90% of them could connect to one access point while only 10% connect to the second access point. This would create a throughput restriction on the access point serving the larger number of clients.

– **Publicly Secure Packet Forwarding** (PSPF) prevents client devices associated with an access point from inadvertently sharing files or communicating with other client devices associated to the access point. To prevent inter-client communications, click the “Enable” radio button.

4.12 Client Configuration

4.12.1 General

To configure the client, click on “Configuration… Client Radio… General” in the left navigation column.

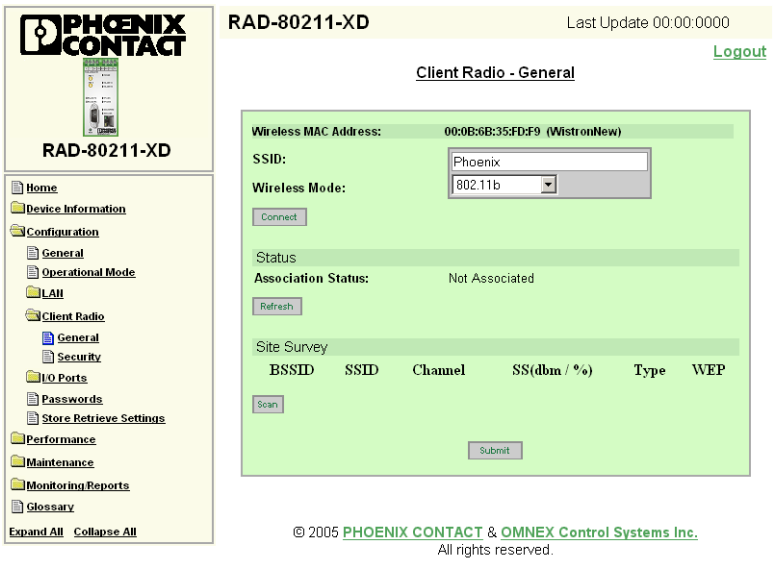


Figure 4-19 “Client Radio - Settings” screen

The buttons and fields in this window are:

– **SSID** defines the SSID of the access point to associate with.
– **Wireless Mode** selects the wireless mode the access point is using. After selecting the wireless mode from the drop-down list, click the “Connect” button and the client will attempt to connect to the access point. Click the “Refresh” button to update the Link Status.
– The **Scan** button causes the radio to do a site survey of the selected “Wireless Mode” to see what access point radios are present and display some basic information on each network.

When the configuration parameters are changed, communication with other radios will be interrupted for 2 to 4 seconds.

4.12.2 Security

To adjust security parameters, click on “Configuration… Client Radio… Security” in the left navigation column.

Open or Shared Authentication (WEP Security)

From the “Authentication Type” drop-down menu, select **Open** or **Shared**. This selection must match the setting in the access point radio. Note that access point radios may be set to allow both.

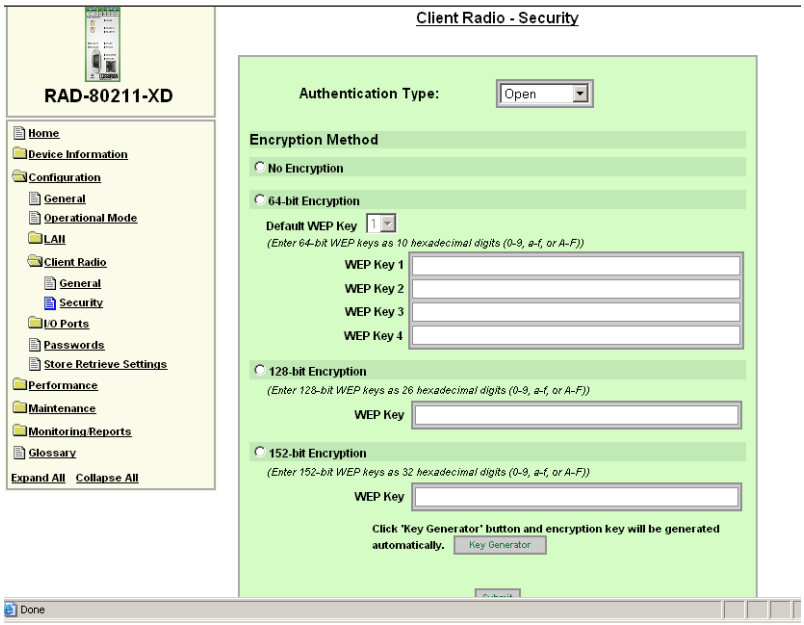


Figure 4-20 “Client Radio - Security” screen

Select a radio button for the number of bits (None, 64, 128 or 152) to be used for security (must be the same as that specified for access point).

Then enter the same WEP Key text (passphrase) as that used for access point. Alternately, you could select Key Generator to have the device automatically generate a key; however, this key must match the access point.

There are four possible keys that can be used with 64-bit encryption. This serves the purpose of allowing periodic rotation of the WEP key by the operator. Simply select which key is desired. The same key must be chosen in the access point and all clients for successful operation. Only one key will be used at a time.

WPA-PSK, WPA2-PSK Encryption and WPA-EAP-TSL, WPA2-EAP-TSL

Enter the “Passphrase” and “Encryption Method” to match the access point. Then click the “Submit” button. If there is a security mismatch between the client and access point, the client will NOT be able to connect to the access point. For additional information about WPA-EAP-TLS security, see “Access Point Security ” on page 4-15.

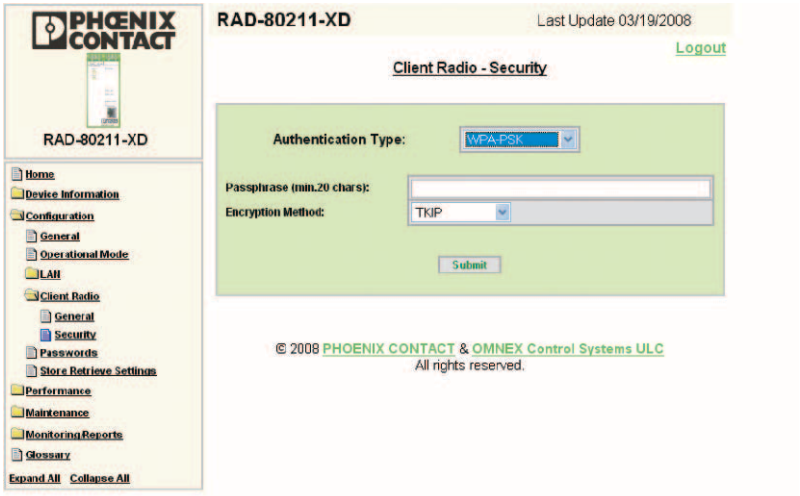


Figure 4-21 “Passphrase and Encryption Method” screen

From the “Authenitication Type” drop-down menu, select **WPA-EAP-TLS**. Then click the “Load New Certificates” button.

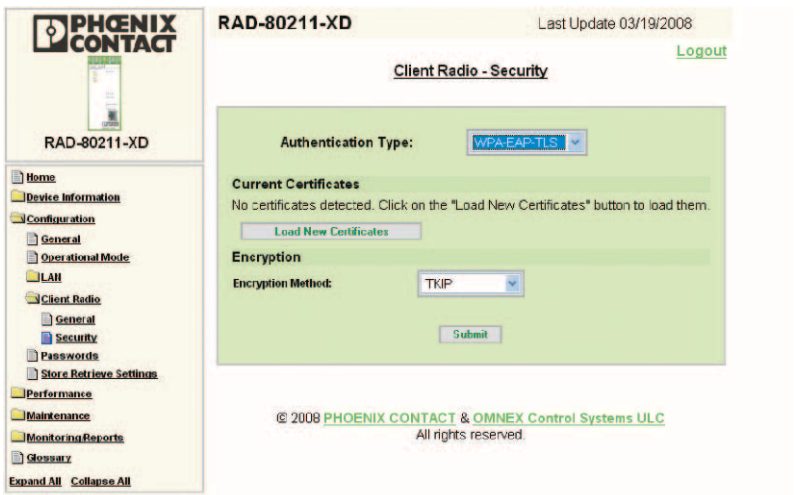


Figure 4-22 Passphrase and Encryption Method for WPA-EAP-TLS Screen

The certificates should be provided by your IT department or network security administrator. After completion of all text fields as shown in Figure 4-23, click the “Update Certs” button.

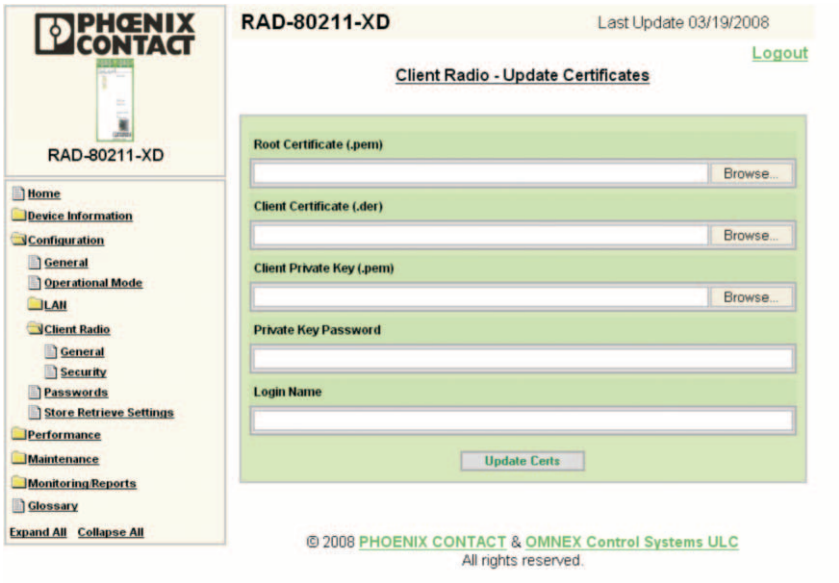


Figure 4-23 Entering Security Titles (New or Updated)

From the drop-down menu, select the encryption method (see Figure 4-24). Encryption method selected must match that used for Access Point. If there is a encryption mismatch between client and AP, the client will NOT be able to connect to the AP. Then click on the Submit button.

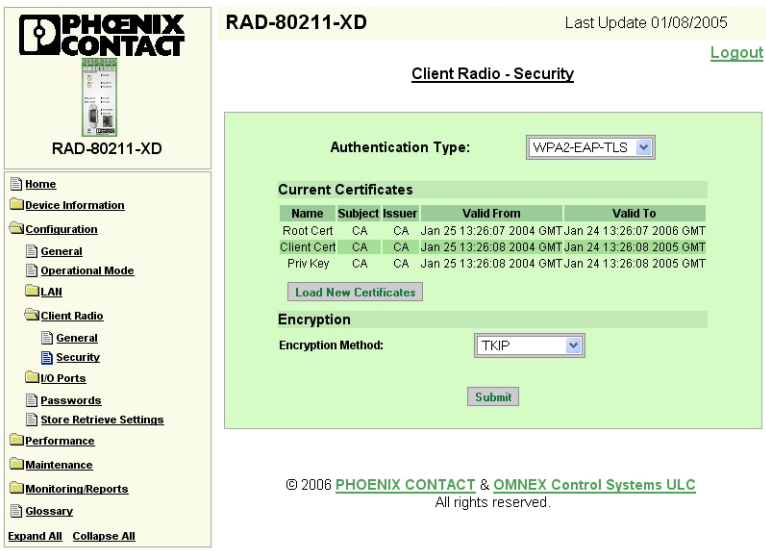


Figure 4-24 Selecting Encryption Method for WPA-EAP-TLS

4.13 Bridge Configuration

4.13.1 General

To configure the bridge, click on “Configuration… Bridge Radio… General” in the left navigation column.

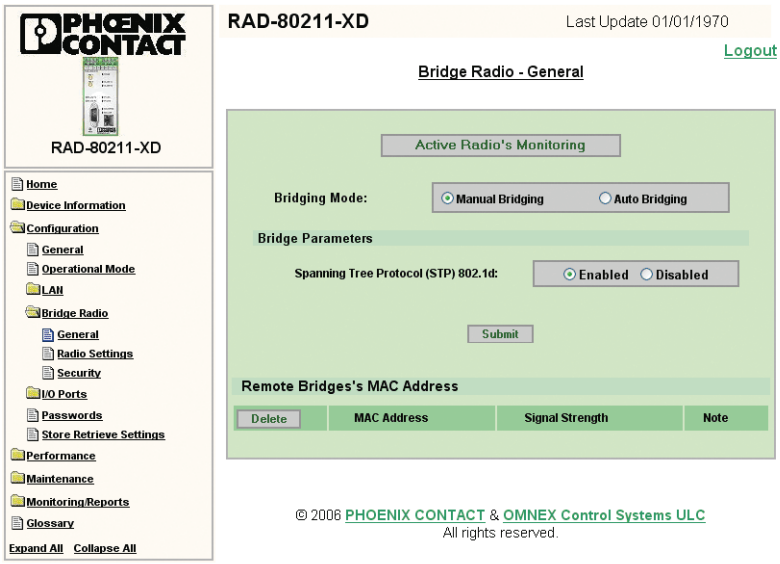


Figure 4-25 “Bridge Radio - General” screen showing Manual Bridging options

Two types of bridging are available: Manual Bridging and Auto Bridging. Click on the appropriate radio button to chose the type of bridging desired. The options available will change to match the type of bridging chosen.

4.13.2 Manual Bridging

The buttons and fields in this window are:

– **Spanning Tree Protocol (IEEE 802.10)** is for radios that are configured in a ring topology. Click the “Enable” button to prevent data from going in an endless cycle around the ring, which can stop communications.

  For ease of installation, the spanning tree protocol (STP) parameters are fixed. The STP parameters are as follows:

Maximum age of STP	20 seconds
Hello time	2 seconds
Forwarding time	2 seconds

  The unit is configured with a priority of 128 with all WLAN units. The lowest MAC address will be the rootswitch, which contains all the STP functions of the system. If other managed switches or routers are to be the root, their priority must be set to lower than 128.

Click the “Active Radio’s Monitoring” button to scan the spectrum and display any networks that are operating within range along with some basic information about the network.

When the configuration parameters are changed, communication with other radios will be interrupted for 2 to 4 seconds.

4.13.3 Auto Bridging

Auto Bridging is an extension of the existing bridge function that is available within the Ethernet radios which simplifies setup, increases robustness, and allows for easier radio replacement within a Phoenix Contact bridge radio network.

NOTE:
With the release of firmware version 2.5.2, Auto Bridging is available in the RAD-80211-XD or RAD-80211-XD-BUS radios. Only radios with HW01 can be upgraded to firmware 2.5.2.

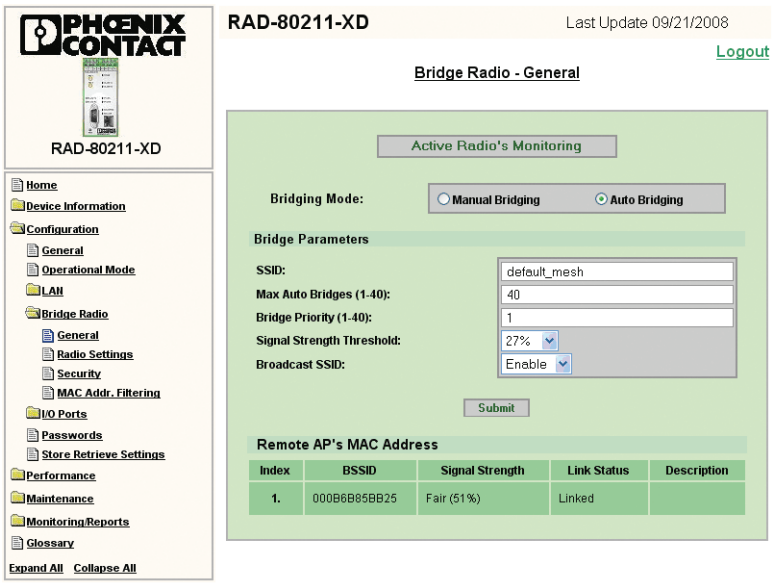


Figure 4-26 “Bridge Radio - Settings” screen showing Auto Bridging options

The “Auto Bridging” function allows RAD-80211-XD or RAD-80211-XD-BUS radios to self-create a bridge radio network with up to 40 radios. The self-created network is defined by an **SSID**, **WLAN Channel** and **Encryption Key** which must be common to all radios within the network. The SSID is the “name” of the wireless network and easily allows new radios to be added or allows for existing radios to change networks by editing a single system parameter.

To create the network, two priority variables are used: **Bridge Priority** and **Signal Strength Threshold**. The Bridge Priority value defines the Root Bridge of the STP-based wireless network. The Root Bridge of the network looks for loops and creates breakpoints to ensure that data flows properly over the wired and wireless infrastructure. Set the Bridge priority value to a low number, such as 1, for the device that is connected to the wired network. This lets all other wireless devices in the network funnel data to that device. In a

simple, wireless network where each remote radio has only a single device connected, it is advisable to set the Bridge Priority value to the same number in all devices (except the Root Bridge device).

The auto bridge function requires that Spanning Tree Protocol (STP) redundancy is enabled. The default setting for STP is enabled. If STP has been previously disabled, click the “Manual Bridging” radio button, and then click the “STP” radio button. To return to Auto Bridging, click the “Auto Bridging” radio button and the STP setting will apply. Failure to set STP will cause network communications to stop.

The Signal Strength Threshold is a minimum value of signal strength that must be achievable in the RF path in order for the link to be created. The threshold can be set to different values for different radios in the network. In order to maintain network stability, the links are monitored for signal degradation or additional paths every 10 seconds. New links are not formed unless the prior link is completely broken, which avoids links constantly making or breaking if the signal strength fluctuates around the threshold.

Once the paths are formed, a calculation places a score on each individual point-to-point link within the mesh.

SS >= Excellent: 100
Excellent > SS >= Good: 400
Good > SS >= Fair: 1600
Fair > SS: 8100

If multiple paths exist from an end device to the root bridge, the scores from each link are added and the path with the lowest score is used. Thus, the network prefers wireless links with strong signals to those without. For example, a path with one “Good” link receives a score of 400 and is preferable to a path with five “Excellent” links with a total score of 500.

To automatically configure the bridge radio settings, click on “Configuration… Bridge Radio… General” in the left navigation column.

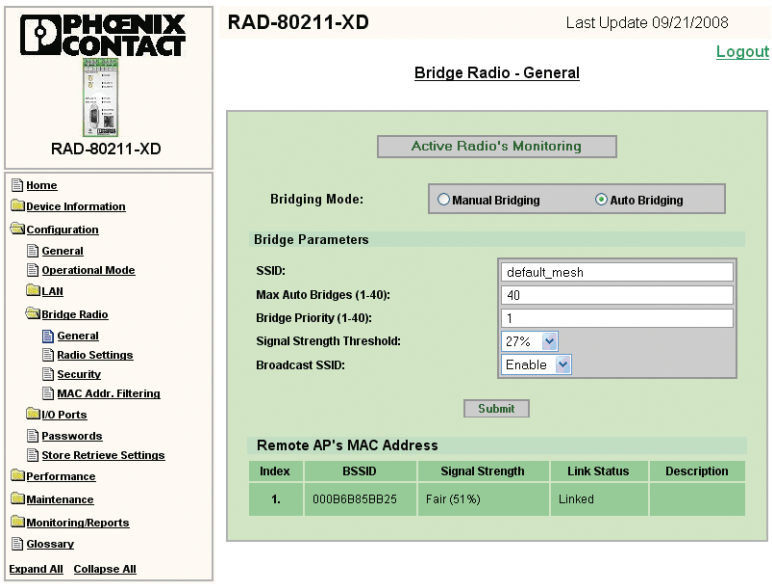


Figure 4-27 “Bridge Radio - Settings” screen

From this screen traditional bridging can be selected by clicking the radio button “Manual Bridging” and automatic bridging can be selected by clicking the “Auto Bridging” radio button.

When auto bridging is selected there are a number of fields that become visible, such as **SSID**, **Max Auto Bridges**, **Bridge Priority**, **Signal Strength Threshold**, and **Broadcast SSID**.

– **SSID**: Service Set IDentifier of the device. This defines which wireless “Auto Bridge” network the radio will communicate with
– **Max. Auto Bridges (1-40)**: Defines the maximum number of Auto Bridging devices allowed to connect to a network. This parameter should remain constant throughout the network.
– **Bridge Priority (1-40)**: Defines the priority of each auto bridging device on the network. Bridge priorities range from 1 to 40, which are actually converted to a range of 257 ~ 296 for 802.1d STP; the lower the value, the higher the importance. In a typical Ethernet switch, the 802.1d bridge priority default is 32768.

The default Bridge priority is 40 (= 296). When connecting a managed switch to an Auto bridged Ethernet radio's RJ45 port and the switch is to be the root switch, its bridge priority must be set to 256 if the Bridge priority of the radio is set to its lowest (a priority of 1 = 257). The root switch in the network must be configured with the lowest Bridge priority.

– **Signal Strength Threshold**: Defines the minimum signal strength allowed for each Auto Bridging device before it must find another path to transfer data. Options are 27%, 21%, 15%, 9% and None.
– **Broadcast SSID**: Defines whether the SSID is being broadcasted across the network or not.

4.13.4 Bridge Radio Settings

To configure the bridge radio settings, click on “Configuration… Bridge Radio… Radio Settings” in the left navigation column.

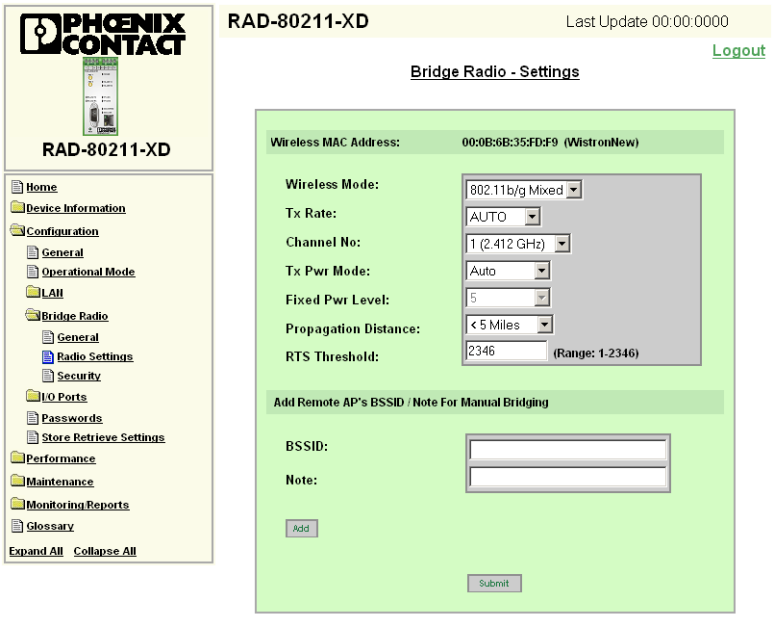


Figure 4-28 “Bridge Radio - Settings” screen

The fields in this screen are:

– Set the “Wireless Mode,” “Tx Rate” and “Channel Number” fields to match the other bridge this radio is communicating with. Adjust the “Tx Pwr Mode” field or leave it set to “Auto” to have the radio calculate how much power is needed to communicate with the remote radio(s).
  – **Wireless Mode** selects a desired wireless mode. Select 802.11a if using only 802.11a clients in the 5 GHz band. This will provide a stronger wireless network if there are existing 802.11b/g networks in the area, or there are other nearby sources of interference in the 2.4 GHz band. 802.11a and g have higher throughput than 802.11b (54 Mbps compared to 11 Mbps).
  – **Channel Number** specifies one of 11 channels available to use in the 2.4 GHz band (802.11b/g). Refer to Figure 4-12 on page 4-13. All of the channels overlap with the exception of 1, 6 and 11. Separate wireless networks should use different channels, preferably non-overlapping. All radios in a wireless network must use the same channel.

    If 802.11a is selected, there are eight non-overlapping channels to choose from: 52, 56, 60, 64, 149, 153, 157, and 161. Refer to Figure 5-13 in this section.

  If uncertain about which channel to use, click the “Select the Optimal Channel” (in 802.11b or g modes only) to let the radio scan for the channel with the least amount of interference. Clients will automatically determine which channel the access point is operating on.

– **Tx Power Mode** sets the transmit power or lets the radio determine how much power is necessary to communicate with the clients. In “Auto” mode, the access point radio will monitor the signal strength from the client. If it begins to get weak, it will automatically boost the transmit power. This works well with mobile clients. Note that the client must have the same amount of transmit power/antenna gain in order to send information back to the access point radio. The range will be dictated by the radio with the least amount of transmit power.
– **Propagation Distance** set this according to how far apart the radios are located. This setting adjusts the amount of time a radio waits to receive a transmission due to propagation delay as it increases with distance.
– **RTS Threshold** is the number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.

4.13.5 Bridge Security

To configure the bridge radio settings, click on “Configuration… Bridge Radio… Security” in the left navigation column.

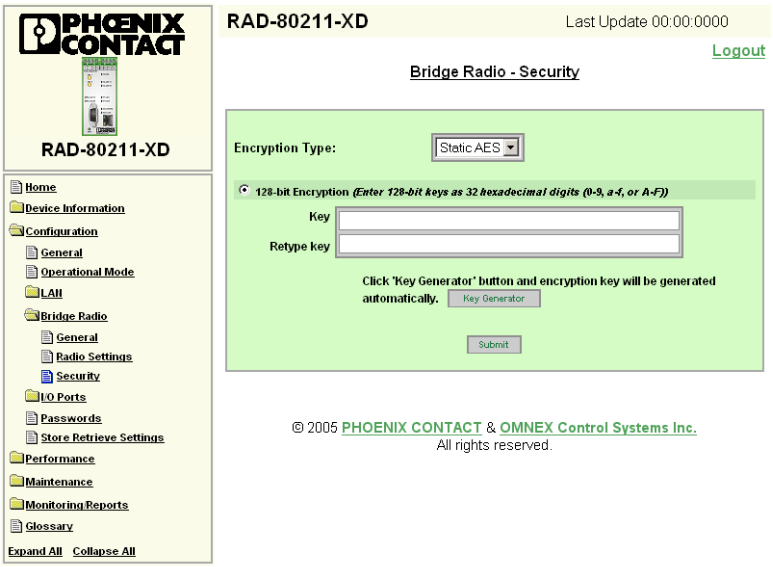


Figure 4-29 “Bridge Radio - Security” screen

The buttons and fields in this window are:

– **Static AES Security** is available from the “Encryption Type” drop-down menu. Enter a 32-digit hexadecimal “Key” or click the “Key Generator” button to have the program generate a key automatically. Copy the key into all other bridge mode radios. All radios on a network must have the same key in order to communicate.

4.14 I/O Ports

4.14.1 Ethernet Port

The Ethernet port settings are only available in radios that are configured as access points or bridges. To configure the Ethernet ports, click on “Configuration… I/O Ports… Ethernet Ports” in the left navigation column. Two advanced functions are available.

Gateway/Ethernet Terminal Radio

Enabling this feature allows data on the Ethernet port of the access point or bridge radio to be redirected to the serial port(s) of the client or remote bridge radios. In Bridge mode, only one radio may be configured as the gateway.

Enter a port number in the “Ethernet Terminal Port Parameters” field. The port number selected is usually determined by the application used to communicate with the Ethernet terminal. Select either TCP or UDP from the “Protocol type” drop-down menu, depending on which protocol the serial data will be packaged with.

Select one of the two Serial Channels from the “Connect to Stream” drop-down menu. This channel must be different from the one used for the Modbus/TCP gateway, if implemented. The same serial channel must be selected when configuring the RS-232 or RS-422/485 port(s) on the remote radio(s).

Modbus/TCP Gateway

Enabling this feature allows radios in access point or bridge mode to emulate a Modbus TCP to Modbus RTU converter. Modbus TCP data packets from the Ethernet port of the access point or bridge will be converted to Modbus RTU packets and redirected out the serial port(s) of the client or remote bridge radios (see Figure 4-30). This mode must be enabled to communicate with the I/O modules on a RAD-80211-XD-BUS radio. In Bridge mode, only one radio may be configured as the gateway. Under “Modbus TCP Parameters”, select 502 as the Port Number.

From the “Modbus Gateway” drop-down menu click the “Network Gateway” option. In the “Connect to Stream” field select one of the two serial channels. Note which serial channel is assigned for Modbus communications. This same serial channel must be assigned to the RS-232, RS-422/485 or I/O port on all remote radios. Click the “Submit” button.

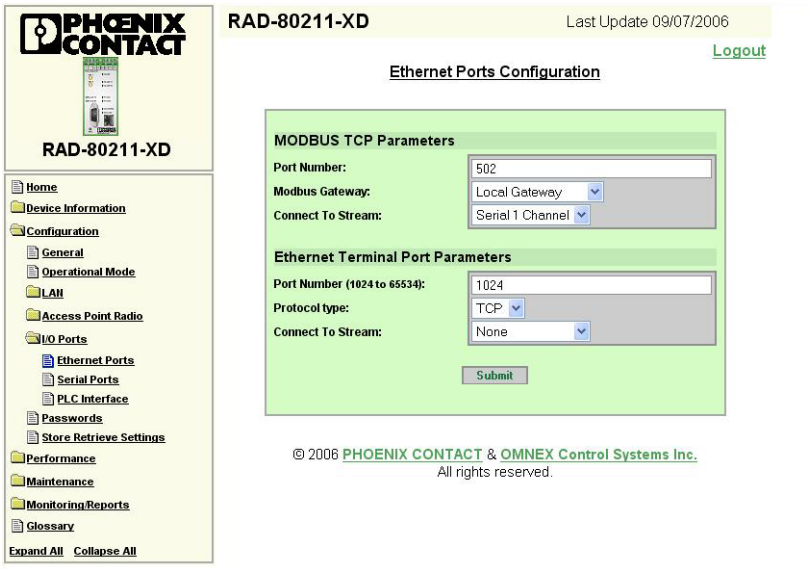


Figure 4-30 “Ethernet Ports Configuration” screen

4.14.2 Serial Ports

There are two independent serial channels available that allow use of the two physical serial ports on each radio (RS-232 and a RS-422/485 port). The serial port function varies depending on the radio mode of operation. Serial data transmitted from a client will only be available at the serial port of the access point. Serial data transmitted from an access point will appear at the serial port of each client (broadcast mode). Data sent into a bridge will be transmitted to the other bridge. If the radios are configured as multipoint bridges, all serial data received by any one bridge will be broadcast to all the other bridges.

To configure the RS-232 or 422/485 ports, click on “Configuration… I/O Port… Serial Ports” in the left navigation column. The screen lists the parameters for either RS-232 or RS-422/485. The settings selected in the “Baud Rate”, “Data Bits”, “Stop Bits”, “Parity”, and “Flow Control” fields must match those of the serial device that will be connected.

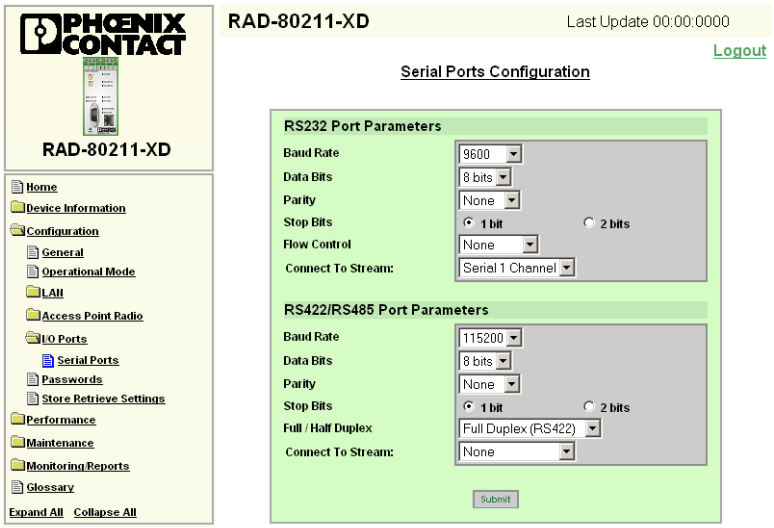


Figure 4-31 “Serial Ports Configuration” screen

- **Baud Rate** refers to the speed data will flow in/out the serial port.
- **Data Bits** refers to how many bits make up each character.
- **Stop Bits** refers to how many bits will signify the end of a character.
- **Parity** is an error checking method.
- **Flow Control** is used to prevent buffer overflow when data streaming into the radio arrives faster than it can be sent out the serial port. The radios have a 600 byte buffer. Buffer overflow occurs when transmitting a message larger than 600 bytes because the over-the-air data rate is much higher than the serial port data rate. Enable flow control to resolve this.
- **Connect to Stream** specifies which of two independent serial channels to use. Each radio has two physical serial ports (RS-232 and a RS-422/485 port). Select one of the two available streams to use. The radio can also be configured as a Modbus/TCP client. It will accept Modbus/TCP requests and convert them to Modbus RTU. The Modbus RTU requests will then be sent out of the serial port. If a serial port is not enabled on the client radio, the Modbus requests will be ignored.

4.14.3 PLC Interface (RAD-80211-XD-BUS only)

RAD-80211-XD-BUS radios allow up to eight RAD I/O modules to be controlled by a Modbus-based (RTU or TCP) PLC/PC or other Modbus Master device. The PLC interface page is used to configure communication parameters associated with the use of the RAD I/O. Refer to Section 5, “XD-BUS Configuration for I/O Modules (RAD-80211-XD-BUS only)” for complete system and configuration information.

4.15 Passwords

There are administrator passwords and monitor passwords. The administrator can make changes to the configuration whereas a monitor can only view information.

To change or set passwords, click on “Configuration… Passwords” in the left navigation column.

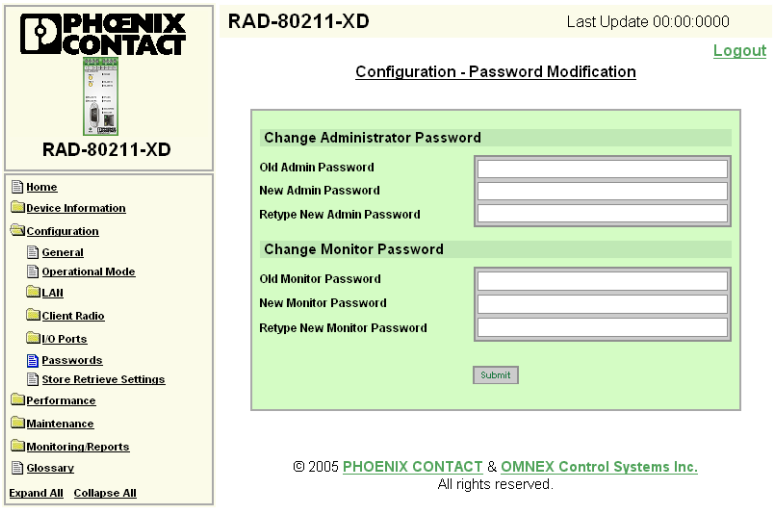


Figure 4-32 “Configuration - Password Modification” screen

4.16 Store and Retrieve Settings

The “Configuration - Store Retrieve Settings” screen allows loading the factory default parameters, saving configuration parameters to a PC’s hard drive and sending the configuration to the radio. To access these functions, click on “Configuration… Store Retrieve Settings” in the left navigation column.

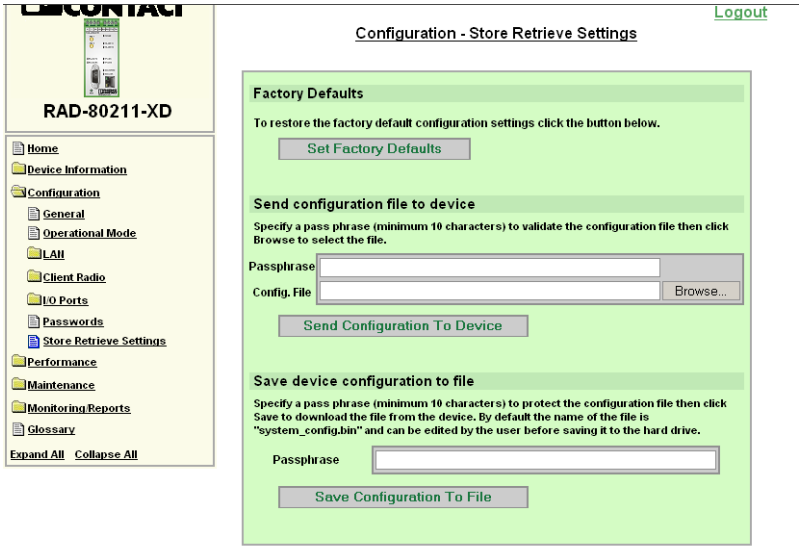

RAD-80211-XD
Home
Device Information
Configuration
General
Operational Mode
LAN
Client Radio
I/O Ports
Passwords
Store Retrieve Settings
Performance
Maintenance
Monitoring/Reports
Glossary
Expand All
Collapse All
Logout
Configuration - Store Retrieve Settings
Factory Defaults
To restore the factory default configuration settings click the button below.
Set Factory Defaults
Send configuration file to device
Specify a pass phrase (minimum 10 characters) to validate the configuration file then click Browse to select the file.
Passphrase
Config. File
Browse...
Send Configuration To Device
Save device configuration to file
Specify a pass phrase (minimum 10 characters) to protect the configuration file then click Save to download the file from the device. By default the name of the file is "system_config.bin" and can be edited by the user before saving it to the hard drive.
Passphrase
Save Configuration To File

Figure 4-33 “Configuration – Store Retrieve Settings” screen

A passphrase is required to protect/validate the file before it can be saved or retrieved from a PC. It prevents unauthorized users from applying the system configuration file to an unauthorized access point to gain access to the network.

4.17 Performance

Several aspects of the device's performance can be monitored. **LAN Performance** provides information on how the Ethernet network is operating. The **Radio Performance** section offers data on how well the information is being transmitted over the air. The **Serial Port** section presents statistics on the RS-232/422/485 data. To access this information, click on "Configuration… Performance" in the left navigation column. Each section contains a dialog box to set the refresh interval (in seconds) of the page.

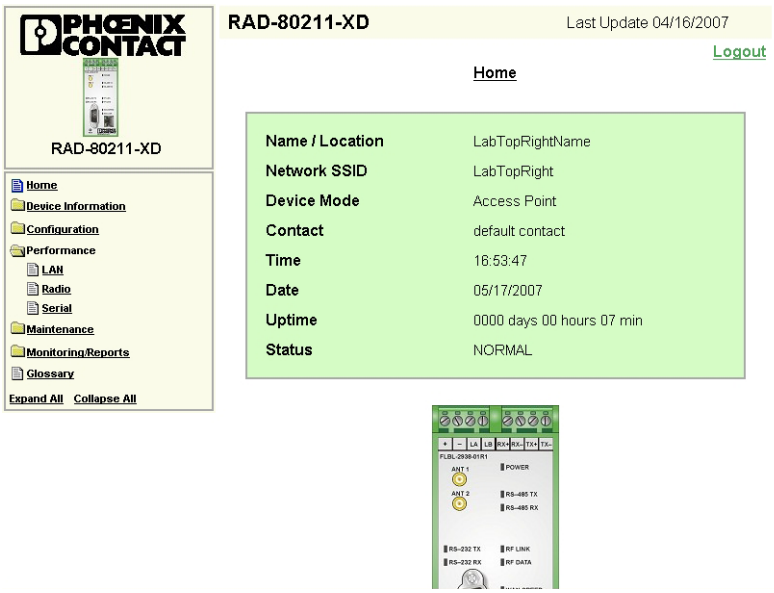


Figure 4-34 "Home" screen with performance options in the left navigation column

4.18 Maintenance

Various maintenance screens are available.

Click on "Maintenance… Register for Updates" in the left navigation column to send an e-mail address to Phoenix Contact. When firmware upgrades become available an e-mail notification will be sent to the registered e-mail address.

Click on "Maintenance…Software Updates" to view the current version of firmware and install new firmware, if available.

Click on "Maintenance… Network Utilities" in the left navigation column to access network commands. Options are available to ping an IP address or host name to find out if it is online and functional as well as perform a "traceroute" command to show the path a packet of information takes to get to its destination.

4.18.1 Software Updates

Click on “Maintenance… Software Updates” in the left navigation column to view the current version of firmware and install a new version (see Figure 4-35).

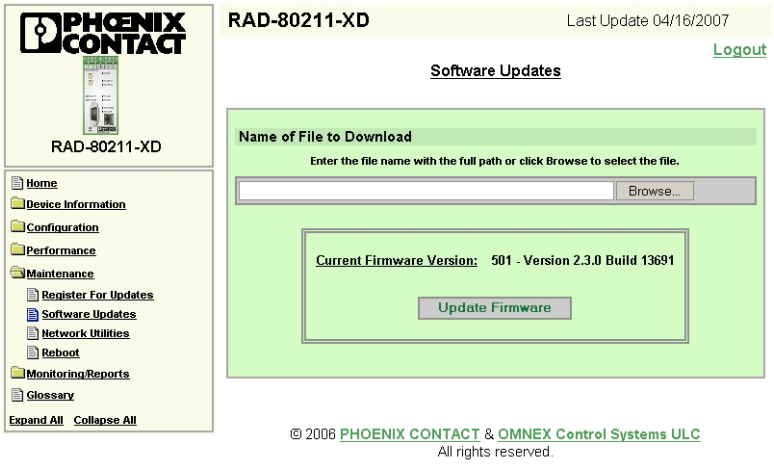


Figure 4-35 “Maintenance… Software Updates” screen

Two different hardware versions exist. Firmware must be compatible with the hardware platform to function correctly as shown Table 4-1.

Table 4-1 Hardware and Firmware Updates

Hardware version [1]	Firmware version
HW00	2.4.x and earlier
HW01	2.5.x and later

1 The hardware version is printed on the label.

To install a new version of firmware, download the firmware to a local drive on the connected computer. Enter the file path in the field or click the “Browse” button to locate the file. Click the “Update Firmware” button to install the update. Follow the messages that appear during the update process.

Any configuration parameters previously entered should remain as configured after the update. Any new features will need to be configured.

4.19 Monitoring/Reports

Click on “Monitoring/Reports” in the left navigation column to access a variety of report screens. These screens allows viewing of the “Web Access Log”, “Bridging Status”, “Site Map”, “System Log” and, if operating in “access point mode”, access to the “AP Client List”, “Adjacent AP List” and “DHCP Server Status” report screens.

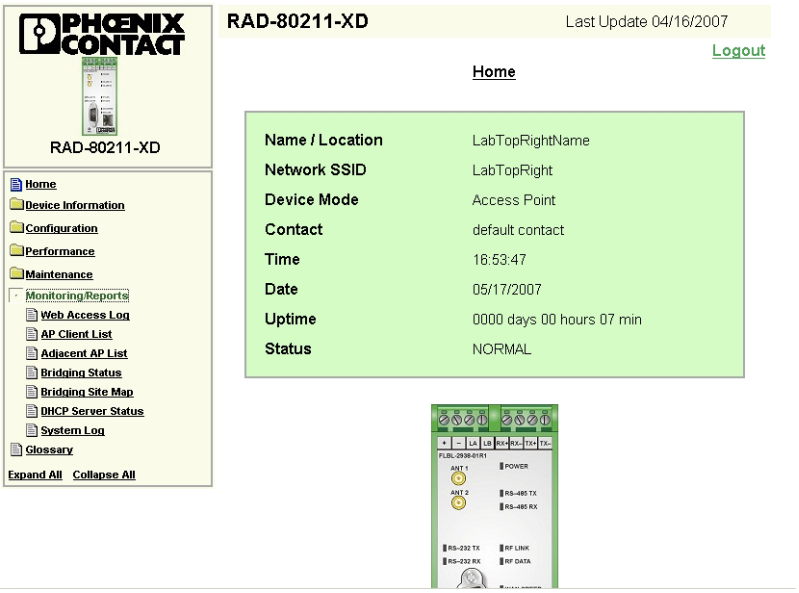


Figure 4-36 “Home” screen with monitoring/report options in the left navigation column

The “Web Access Log” displays system facility messages with date and time stamp for any actions involving web access. For example, this log records when the encryption mode was set, if the operating mode was changed, etc., using the web browser. The log also documents the user who made the changes. The Web Access Log will continue to accumulate listings. To clear the listings, use the “Clear” button.

The “Bridging Status” and “Bridge Site Map” provide statistics on a bridge connection.

“System Log” records all processes within the radio. It is used primarily for debugging.

The “AP Client List” shows all clients that are connected to this access point.

The “Adjacent AP List” shows all access points that are within range of this access point. Selecting an access point and clicking the “Trust” button adds that access point to the list of trusted access points. This prevents an access point from being reported as a rogue access point.

Section 5

This section informs you about

- RAD I/O communications
- I/O Module descriptions
- Addressing remote I/O
- Rotary switches
- Register scaling
- Wiring and Fail Condition DIP switches
- Accessing the XML file

XD-BUS Configuration for I/O Modules (RAD-80211-XD-BUS only) 5-3

5.1 I/O Communications 5-3
5.1.1 Modbus TCP I/O Emulation Operation 5-3
5.1.2 System Overview 5-3
5.1.3 I/O System Configuration Overview 5-4
5.1.4 Configuring the Radio to Connect to the I/O Modules 5-4
5.1.5 Configuring Radios Connected to the PLC /Modbus Master 5-7

5.2 I/O Module Descriptions 5-8
5.2.1 Connecting and Configuring the I/O Modules 5-9

5.3 Addressing the Remote I/O 5-9

5.4 Rotary Switches 5-15

5.5 Register Scaling 5-15
5.5.1 Digital Channels 5-15
5.5.2 Analog Channel Scaling 5-16
5.5.3 Pulse Input Channels 5-16
5.5.4 Pulse Output Channels 5-16

5.6 Wiring and Fail Condition DIP Switches for the I/O Modules 5-18
5.6.1 Analog Input Module 5-18
5.6.2 Digital Input Module 5-19
5.6.3 Analog Output Module 5-20
5.6.4 Digital Output Module 5-21
5.6.5 Combination Input/Output Module 5-22
5.6.6 Digital Pulse Input Module 5-23
5.6.7 Digital Pulse Output Module 5-26

5.7 Accessing the XML file 5-28

5 XD-BUS Configuration for I/O Modules (RAD-80211-XD-BUS only)

5.1 I/O Communications

5.1.1 Modbus TCP I/O Emulation Operation

Modbus TCP data is sent into the radio configured as the Modbus Gateway. The data is directed to a specific TCP port number (502 for Modbus). This data is then converted to Modbus RTU protocol and sent to all other radios in the network on one of the two available serial streams. At the remote radios, the Modbus packets are sent to the I/O ports (RS-232, RS-422/485 or the I/O modules) that are assigned to that serial stream.

If the serial stream is assigned to I/O modules on a RAD-80211-XD-BUS and the Modbus node address of the radio matches that in the packet, a standard Modbus RTU response packet will be generated. The analog I/O values are stored in the 4xxxx registers, the digital input values are stored in the 1xxxx series registers, and the digital outputs are controlled by writing to the 0xxxx registers. The 8-position rotary switch on the top of each I/O module influences which register each module's I/O will be located. See Tables 6-1 and 6-2.

When a Modbus RTU response packet is received at the access point or local bridge radio, the radio converts the Modbus RTU packet back into a Modbus/TCP packet and sends the data through the Ethernet port to the host device.

5.1.2 System Overview

The RAD-80211-XD-BUS radios allow up to eight RAD I/O modules to be controlled by a Modbus (RTU or TCP) based PLC/PC (or other Modbus master device). The group of RAD I/O modules, connected to a RAD-80211-XD-BUS radio, act as a single Modbus slave I/O station, and communicate over a wired or wireless serial communications stream to a Modbus TCP or Modbus RTU master PLC (or other type of controlling device).

Typical I/O Applications

Many application configurations are possible including the following:

1. Master PLC connected to any RAD-80211-XD... radio and configured either as an access point or bridge. Configured as wireless, the master PLC controls RAD I/O attached to remotely mounted RAD-80211-XD-BUS radios (client mode).
   - Master PLC connects to the radio's serial port and uses Modbus RTU.
   - Master PLC connects to the radio's Ethernet port and uses Modbus TCP.
2. Master PLC connected to a RAD-80211-XD-BUS radio and configured either as an access point or bridge radio. The master PLC controls both locally attached RAD I/O and, over wireless, controls I/O attached to remotely mounted RAD-80211-XD-BUS radios (client mode).
   - Master PLC connects to the radio's serial port and uses Modbus RTU
   - Master PLC connects to the radio's Ethernet port and uses Modbus TCP

Additional System Flexibility

1. Any RAD-80211-XD... radio can be used in applications where a master PLC communicates wirelessly to distributed PLCs that are attached to remotely mounted RAD-80211-XD... radio members.
2. While I/O communication uses one of the two serial communication streams, the other stream may be used simultaneously with other devices connected to the unused serial and Ethernet ports.

5.1.3 I/O System Configuration Overview

To enable communications between the RAD I/O and a Modbus based master, the following radio settings need to be configured.

1. RAD-80211-XD-BUS radio connected to the I/O:
   a) The Modbus address and communications time out of the RAD-80211-XD-BUS radio must be set.
   b) The I/O must be assigned to the serial communications stream that will be controlling them.

NOTE:
For applications where a single master is polling multiple RAD-80211-XD-BUS-based I/O stations, all the I/O stations must be set to the same serial communications stream.

   c) When the I/O is used as a stand-alone remote I/O station, the radio is typically configured as a client.
   d) If the PLC/Modbus master connects to a RAD-80211-XD-BUS radio in order to use its I/O as additional locally mounted I/O, the radio can be configured as a wireless access point or a bridge mode. In this case the radio's master settings must also be configured (see "Typical I/O Applications" on page 5-3).
2. Any RAD-80211-XD... radio connected to the PLC /Modbus master:
   a) The serial (RS-232) port or Ethernet port connected to the Modbus master must be assigned to a serial communications stream.
   b) If the master is a Modbus TCP (Ethernet) device, the Modbus gateway function must be enabled. This converts the Modbus TCP commands to the Modbus RTU commands. These commands are used by the RAD-80211-XD-BUS unit to control the I/O. The communication conversion is one-way. Only Modbus TCP commands are converted to Modbus RTU commands. A serial Modbus RTU master cannot use the Modbus gateway function to talk to other Modbus TCP based I/O.
   c) The RAD-80211-XD-BUS radio must be configured as either a wireless access point or a bridge mode.

5.1.4 Configuring the Radio to Connect to the I/O Modules

PLC Interface Configuration

To enable communications between the radio and a Modbus based master, three parameters must first be configured: the Modbus address set; Communications Timeout set and; a communications stream assigned. These parameters are found on the PLC Interface Configuration web page. Configure the radio as described in the following steps so that the I/O modules can be accessed.

1. Click on “Configuration… I/O Ports… PLC Interface” in the left navigation column.

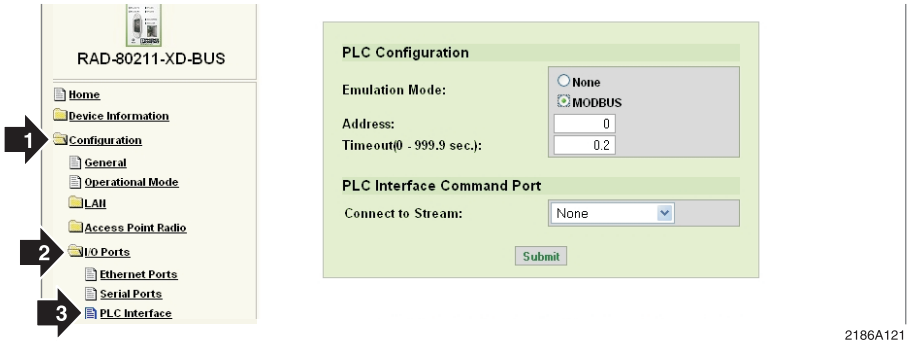


Figure 5-1 “PLC Configuration” screen

2. Set the **Emulation Mode.**
   To enable communications between the RAD-80211-XD-BUS and a Modbus-based master, click the “Modbus” button.
3. Enter the **PLC Address**.
   Enter the desired Modbus node address assigned to the radio. The address should be between **0** and **255** and must be different from all other Modbus devices in the network. A wrong address setting will result in the PLC address box reset to **0**.
4. Enter a **Timeout** value.
   The timeout setting controls a communications watchdog timer that triggers the I/O fault mode in the event communication between the PLC/Modbus master and the I/O are disrupted. The timeout default setting is 0.2 seconds (200 ms). Enter a value between 0.1 and 999.9 seconds. A “0” setting disables the communications watchdog timer. See “Timeout Setting for I/O Control” on page 5-5” for more detailed information.
5. Enter the value to **Connect to a Stream**.
   One of the two serial communication streams must be dedicated to handle the communication to and from the I/O. Select either of the two serial channels. Since only one stream can control all the I/O in the system, the channel selected must be the same for the Modbus master and all I/O connected to all the radios.

Timeout Setting for I/O Control

A communications timeout setting is needed because there can be many intermediate radios or Ethernet segments between the Modbus (RTU or TCP) master device and the various radio’s slave I/O. Due to the multiple intermediate segments, communications can be stopped even though the radio link or Ethernet link to the radio is intact. The timeout function compares the elapsed time between the last Modbus read or write commands and a preset value. If the actual time exceeds the timeout preset, the radio assumes that the I/O modules are no longer under control, and sets all the I/O attached to the radio to their fault state. The value should be set to the slowest machine or process function that the I/O (attached to the radio) is controlling.

I/O Timeout Diagnostics

In the event of a timeout, the STATUS LED flashes (at a fast two flashes per second rate) indicating an “Application Error.” At the same time, the status LEDs on the I/O module(s) will also flash (at a slow one flash per second rate). In addition, the radio sends an Ethernet error message via SNMP and makes an entry into the diagnostic log web page. When communication is re-established by the next Modbus read or write command, the watchdog is reset, I/O communications automatically resume, an **I/O is Operational** SNMP message is sent and a web-based diagnostic log message is entered.

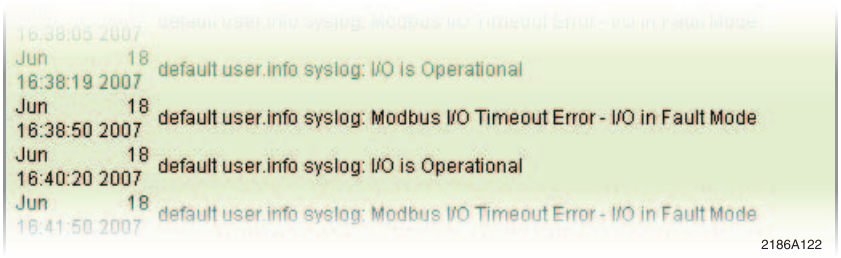

Jun 18 16:38:19 2007
default user.info syslog: I/O is Operational
Jun 18 16:38:50 2007
default user.info syslog: Modbus I/O Timeout Error - I/O in Fault Mode
Jun 18 16:40:20 2007
default user.info syslog: I/O is Operational
Jun 18
default user.info syslog: Modbus I/O Timeout Error - I/O in Fault Mode
2186A122

Figure 5-2 Example of SNMP diagnostic error message

Duplicate I/O Addresses

NOTE:
If I/O modules are installed with duplicate addresses (rotary switch settings), the I/O data will be erroneous. When installing or changing I/O modules, ensure that the status LED’s indicate a valid I/O configuration before reading or writing data to the I/O. Failure to do this may result in unexpected machine or process operation.

Control I/O From One Source

The I/O is designed for control in a typical Modbus (RTU or TCP) master slave system. For proper system operation, only one Modbus RTU or Modbus TCP master is to control the I/O modules and turn on outputs. The RAD-80211-XD-BUS radio is designed to allow the I/O to be controlled from either Ethernet-based Modbus TCP or serial interface based Modbus RTU masters. When assigning the PLC I/O function to a communication stream, ensure that

there is only one source controlling the I/O: either a single Ethernet master source or a single serial source, but NOT both. If two I/O control sources are assigned to the I/O stream, the error message shown in Figure 5-3 is generated.

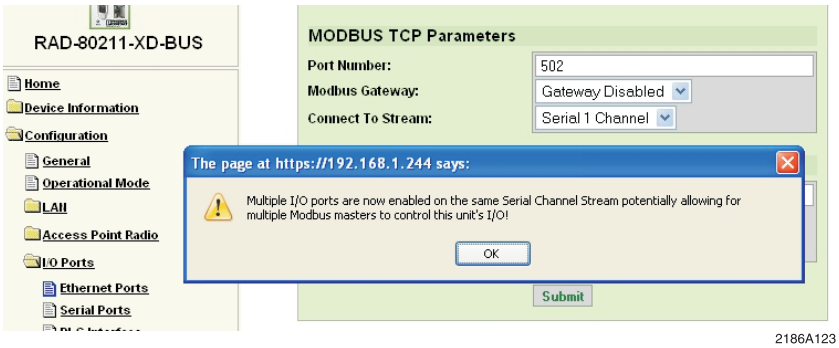


Figure 5-3 Error message – Multiple I/O communication control sources on same channel

WARNING:
Attempting to control the I/O from two or more masters may lead to intermittent control of the outputs, which can cause machine/process damage or personnel injury.

5.1.5 Configuring Radios Connected to the PLC /Modbus Master

General Configuration

To connect a RAD-80211-XD-BUS radio to a Modbus master device – either Modbus RTU serial or Modbus TCP Ethernet-based (i.e., a PLC or PC-based controller), the radio must be configured as an access point or bridge (refer to “General Configuration” on page 4-7.

Configuration When Connecting to a Modbus RTU Master Controller

Modbus RTU masters connect to either the RS-232 or RS-422/485 serial ports on the radio.

1. Configure the serial ports physical parameters (baud rate, stop bits, etc.) (refer to “Serial Ports” on page 4-32).
2. Configure the RAD-80211-XD-BUS communication stream to the same communication stream as that used by the RAD-80211-XD-BUS unit’s I/O (refer to “Serial Ports” on page 4-32).

Configuration When Connecting to a Modbus TCP Ethernet Master Controller

Modbus TCP master devices connect to the Ethernet port on the radio.

1. Configure the Ethernet port’s link speed and duplex settings (refer to “LAN Configuration” on page 4-9)
2. Configure the Modbus Gateway parameter to “Network Gateway” and enter “502” as the port number (refer to “Modbus/TCP Gateway” on page 4-31
3. Configure the RAD-80211-XD-BUS communication stream to the same communication stream as that used by the RAD-80211-XD-BUS unit’s I/O. Refer to “Serial Ports” on page 4-32).

Ensure that there is only one source controlling the I/O: either a single Ethernet master source, or a single serial source, but NOT both on the same communications stream.

WARNING:
Attempting to control the I/O from two or more masters may lead to intermittent control of the outputs, which can cause machine/process damage or personnel injury.

5.2 I/O Module Descriptions

There are seven different I/O modules that can be used with the RAD-80211-XD-BUS radio. They are powered from the radio through the 5-pin male/female connector on either side of the radio and I/O module. They feature an 8-position rotary switch on the top of each module for addressing.

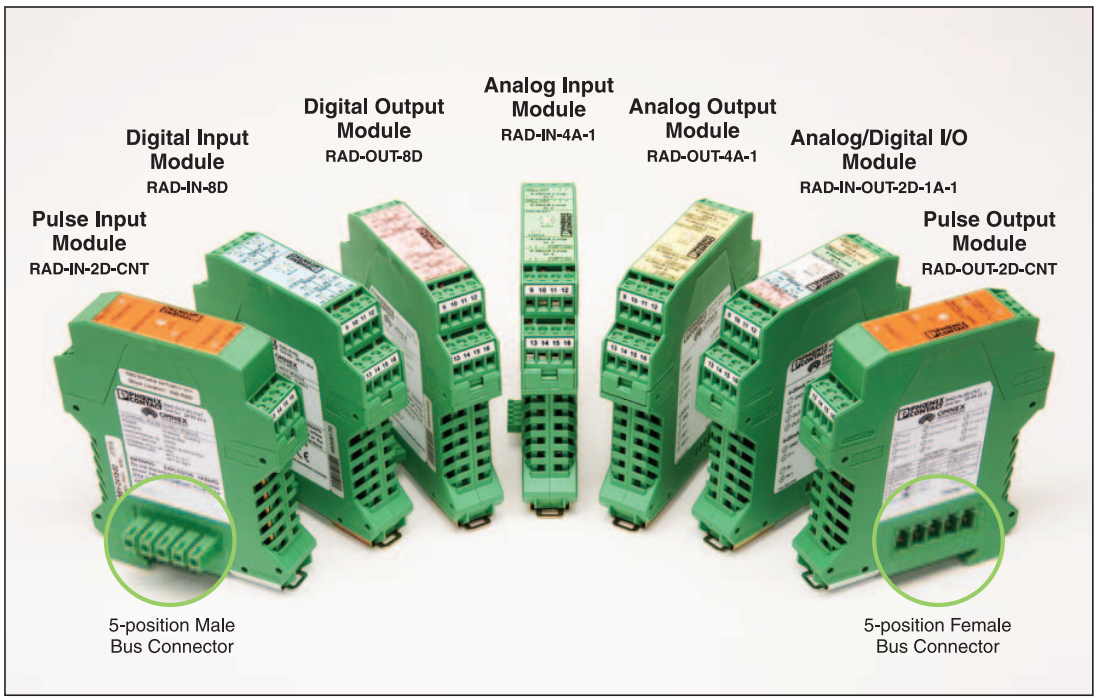


Figure 5-4 I/O modules used with the RAD-80211-XD-BUS

Analog Input Module – RAD-IN-4A-I

This module has four (4) 0-22 mA current inputs. It can accept either powered loops or provide the power for a loop. The power supply for the loops is common to the radio's power supply.

Analog Output Module – RAD-OUT-4A-I

This module has four (4) 0-22 mA current outputs. It can accept either powered loops or provide the power for a loop. Each current loop is optically isolated. Internally there are four DIP switches that determine what happens to each current channel if the radio link is lost – either "fail to 2 mA" or "maintain the last known value."

Digital Input Module – RAD-IN-8D

This module has eight (8) digital inputs. Each input requires a voltage to trigger it. Each channel is optically isolated.

Digital Output Module – RAD-OUT-8D

This module has eight (8) digital outputs. Each output is a normally open dry contact. Internally there are eight DIP switches that determine what happens to each channel if the radio link is lost – either “fail open” or “maintain the last known value.”

Analog/Digital I/O Module – RAD-IN+OUT-2D-1A-I

This module has a mix of inputs and outputs – 1 analog input, 1 analog output, 2 discrete inputs and 2 discrete outputs. Internally there are DIP switches that determine the fail condition of the outputs in a similar fashion as described in the above modules.

Pulse Input Module – RAD-IN-2D-CNT

This module has two configurable pulse or frequency inputs. A 5-position DIP switch inside the module is used to set the mode of each channel, as well as the input impedance, coupling, speed, and input type (single-ended or differential). It is compatible with the following common pulse generating devices.

– AC sine wave output devices such as magnetic transducers.
– Digital pulse output devices such as microprocessor-based flow meters.
– Mechanical relay pulse output devices or toggle switches.

Pulse Output Module – RAD-OUT-2D-CNT

This module has two configurable pulse or frequency outputs. A 4-position DIP switch inside the module is used to set the mode of each channel as well as the speed (high or low).

5.2.1 Connecting and Configuring the I/O Modules

1. Remove the plastic housing from the output modules and set the fail condition DIP switches as desired for each channel (refer to page 5-18 for more details.
2. Connect the I/O modules and radio to the DIN rail and slide them together so the 5-pin male/female connectors mate.
3. Set the 8-position rotary switch on the I/O modules so each I/O module connected to the radio has a unique address.
4. Wire the analog and discrete signals. Next, connect the antenna and apply power.

5.3 Addressing the Remote I/O

Each radio must have a unique Modbus address programmed into it. I/O modules attached to each radio have their analog, discrete, or frequency inputs and outputs mapped to registers. When a command from the master PLC (through the Modbus/TCP Gateway radio) is broadcast to all remote radios, they read the address to determine if they should respond. Within each command there will be a read or write request to certain registers. Table 5-1 and Table 5-2 are address maps that correlate each I/O channel to a Modbus register.

Note that the initial register shows the RSSI. The RSSI is presented as a positive number. Add the negative sign to determine the RSSI in –dB. For example, if 67 is the value in decimal in the register, the RSSI is –67dB. Note that this information is only available on remote radios. The Gateway or Ethernet Terminal radio will not provide this information.

Table 5-1 MODBUS Memory Map

	0	10000	40000
1	Reserved	Reserved	RSSI
2	Reserved	Reserved	Reserved
3	Reserved	Reserved	Reserved
4-16	Reserved	Reserved	Reserved
17-24	Module #1 digital outputs	Module #1 digital inputs	Module #1 analog inputs
25-32	Reserved	Reserved	Module #1 analog outputs
33-40	Module #2 digital outputs	Module #2 digital inputs	Module #2 analog inputs
41-48	Reserved	Reserved	Module #2 analog outputs
49-56	Module #3 digital outputs	Module #3 digital inputs	Module #3 analog inputs
57-64	Reserved	Reserved	Module #3 analog outputs
65-72	Module #4 digital outputs	Module #4 digital inputs	Module #4 analog inputs
73-80	Reserved	Reserved	Module #4 analog outputs
81-88	Module #5 digital outputs	Module #5 digital inputs	Module #5 analog inputs
89-96	Reserved	Reserved	Module #5 analog outputs
97-104	Module #6 digital outputs	Module #6 digital inputs	Module #6 analog inputs
105-112	Reserved	Reserved	Module #6 analog outputs
113-120	Module #7 digital outputs	Module #7 digital inputs	Module #7 analog inputs
121-128	Reserved	Reserved	Module #7 analog outputs
129-136	Module #8 digital outputs	Module #8 digital inputs	Module #8 analog inputs
137-144	Reserved	Reserved	Module #8 analog outputs
145	Reserved	Reserved	Reserved
146	Reserved	Reserved	Reserved
147	Reserved	Reserved	Module #1 digital inputs
148	Reserved	Reserved	Module #1 digital outputs
149	Reserved	Reserved	Module #2 digital inputs
150	Reserved	Reserved	Module #2 digital outputs
151	Reserved	Reserved	Module #3 digital inputs
152	Reserved	Reserved	Module #3 digital outputs
153	Reserved	Reserved	Module #4 digital inputs
154	Reserved	Reserved	Module #4 digital outputs
155	Reserved	Reserved	Module #5 digital inputs
156	Reserved	Reserved	Module #5 digital outputs
157	Reserved	Reserved	Module #6 digital inputs
158	Reserved	Reserved	Module #6 digital outputs

Table 5-1 MODBUS Memory Map

	0	10000	40000
159	Reserved	Reserved	Module #7 digital inputs
160	Reserved	Reserved	Module #7 digital outputs
161	Reserved	Reserved	Module #8 digital inputs
162	Reserved	Reserved	Module #8 digital outputs

Modbus Register Addressing
Config Switch No. 4, Switch No. 1=OFF

Table 5-2 Modbus Pulse Memory Map

	0	40000
17	Module #1 Input 1 Value Control Bit	Module #1 Input 1 LSW Value
18	Module #1 Input 2 Value Control Bit	Module #1 Input 1 MSW Value (Pulse mode only)
19		Module #1 Input 1 LSW Value Store (Pulse mode only)
20		Module #1 Input 1 MSW Value Store (Pulse mode only)
21		Module #1 Input 2 LSW Value
22		Module #1 Input 2 MSW Value (Pulse mode only)
23		Module #1 Input 2 LSW Value Store (Pulse mode only)
24		Module #1 Input 2 MSW Value Store (Pulse mode only)
25		Module #1 Output 1 LSW Value
26		Module #1 Output 1 MSW Value (Pulse mode only)
27		Module #1 Output 1 Absolute or Differential Operation LSW
28		Module #1 Output 1 Absolute or Differential Operation MSW
29		Module #1 Output 2 LSW Value
30		Module #1 Output 2 MSW Value (Pulse mode only)
31		Module #1 Output 2 Absolute or Differential Operation LSW
32		Module #1 Output 2 Absolute or Differential Operation MSW
33	Module #2 Input 1 Value Control Bit	Module #2 Input 1 LSW Value
34	Module #2 Input 2 Value Control Bit	Module #2 Input 1 MSW Value (Pulse mode only)
35		Module #2 Input 1 LSW Value Store (Pulse mode only)
36		Module #2 Input 1 MSW Value Store (Pulse mode only)
37		Module #2 Input 2 LSW Value
38		Module #2 Input 2 MSW Value (Pulse mode only)
39		Module #2 Input 2 LSW Value Store (Pulse mode only)
40		Module #2 Input 2 MSW Value Store (Pulse mode only)
41		Module #2 Output 1 LSW Value
42		Module #2 Output 1 MSW Value (Pulse mode only)
43		Module #2 Output 1 Absolute or Differential Operation LSW
44		Module #2 Output 1 Absolute or Differential Operation MSW
45		Module #2 Output 2 LSW Value

Table 5-2 Modbus Pulse Memory Map

	0	40000
46		Module #2 Output 2 MSW Value (Pulse mode only)
47		Module #2 Output 2 Absolute or Differential Operation LSW
48		Module #2 Output 2 Absolute or Differential Operation MSW
49	Module #3 Input 1 Value Control Bit	Module #3 Input 1 LSW Value
50	Module #3 Input 2 Value Control Bit	Module #3 Input 1 MSW Value (Pulse mode only)
51		Module #3 Input 1 LSW Value Store (Pulse mode only)
52		Module #3 Input 1 MSW Value Store (Pulse mode only)
53		Module #3 Input 2 LSW Value
54		Module #3 Input 2 MSW Value (Pulse mode only)
55		Module #3 Input 2 LSW Value Store (Pulse mode only)
56		Module #3 Input 2 MSW Value Store (Pulse mode only)
57		Module #3 Output 1 LSW Value
58		Module #3 Output 1 MSW Value (Pulse mode only)
59		Module #3 Output 1 Absolute or Differential Operation LSW
60		Module #3 Output 1 Absolute or Differential Operation MSW
61		Module #3 Output 2 LSW Value
62		Module #3 Output 2 MSW Value (Pulse mode only)
63		Module #3 Output 2 Absolute or Differential Operation LSW
64		Module #3 Output 2 Absolute or Differential Operation MSW
65	Module #4 Input 1 Value Control Bit	Module #4 Input 1 LSW Value
66	Module #4 Input 2 Value Control Bit	Module #4 Input 1 MSW Value (Pulse mode only)
67		Module #4 Input 1 LSW Value Store (Pulse mode only)
68		Module #4 Input 1 MSW Value Store (Pulse mode only)
69		Module #4 Input 2 LSW Value
70		Module #4 Input 2 MSW Value (Pulse mode only)
71		Module #4 Input 2 LSW Value Store (Pulse mode only)
72		Module #4 Input 2 MSW Value Store (Pulse mode only)
73		Module #4 Output 1 LSW Value
74		Module #4 Output 1 MSW Value (Pulse mode only)
75		Module #4 Output 1 Absolute or Differential Operation LSW
76		Module #4 Output 1 Absolute or Differential Operation MSW
77		Module #4 Output 2 LSW Value
78		Module #4 Output 2 MSW Value (Pulse mode only)
79		Module #4 Output 2 Absolute or Differential Operation LSW
80		Module #4 Output 2 Absolute or Differential Operation MSW
81	Module #5 Input 1 Value Control Bit	Module #5 Input 1 LSW Value
82	Module #5 Input 2 Value Control Bit	Module #5 Input 1 MSW Value (Pulse mode only)
83		Module #5 Input 1 LSW Value Store (Pulse mode only)

Table 5-2 Modbus Pulse Memory Map

	0	40000
84		Module #5 Input 1 MSW Value Store (Pulse mode only)
85		Module #5 Input 2 LSW Value
86		Module #5 Input 2 MSW Value (Pulse mode only)
87		Module #5 Input 2 LSW Value Store (Pulse mode only)
88		Module #5 Input 2 MSW Value Store (Pulse mode only)
89		Module #5 Output 1 LSW Value
90		Module #5 Output 1 MSW Value (Pulse mode only)
91		Module #5 Output 1 Absolute or Differential Operation LSW
92		Module #5 Output 1 Absolute or Differential Operation MSW
93		Module #5 Output 2 LSW Value
94		Module #5 Output 2 MSW Value (Pulse mode only)
95		Module #5 Output 2Absolute or Differential Operation LSW
96		Module #5 Output 2 Absolute or Differential Operation MSW
97	Module #6 Input 1 Value Control Bit	Module #6 Input 1 LSW Value
98	Module #6 Input 2 Value Control Bit	Module #6 Input 1 MSW Value (Pulse mode only)
99		Module #6 Input 1 LSW Value Store (Pulse mode only)
100		Module #6 Input 1 MSW Value Store (Pulse mode only)
101		Module #6 Input 2 LSW Value
102		Module #6 Input 2 MSW Value (Pulse mode only)
103		Module #6 Input 2 LSW Value Store (Pulse mode only)
104		Module #6 Input 2 MSW Value Store (Pulse mode only)
105		Module #6 Output 1 LSW Value
106		Module #6 Output 1 MSW Value (Pulse mode only)
107		Module #6 Output 1 Absolute or Differential Operation LSW
108		Module #6 Output 1 Absolute or Differential Operation MSW
109		Module #6 Output 2 LSW Value
110		Module #6 Output 2 MSW Value (Pulse mode only)
111		Module #6 Output 2 Absolute or Differential Operation LSW
112		Module #6 Output 2 Absolute or Differential Operation MSW
113	Module #7 Input 1 Value Control Bit	Module #7 Input 1 LSW Value
114	Module #7 Input 2 Value Control Bit	Module #7 Input 1 MSW Value (Pulse mode only)
115		Module #7 Input 1 LSW Value Store (Pulse mode only)
116		Module #7 Input 1 MSW Value Store (Pulse mode only)
117		Module #7 Input 2 LSW Value
118		Module #7 Input 2 MSW Value (Pulse mode only)
119		Module #7 Input 2 LSW Value Store (Pulse mode only)
120		Module #7 Input 2 MSW Value Store (Pulse mode only)
121		Module #7 Output 1 LSW Value

Table 5-2 Modbus Pulse Memory Map

	0	40000
122		Module #7 Output 1 MSW Value (Pulse mode only)
123		Module #7 Output 1 Absolute or Differential Operation LSW
124		Module #7 Output 1 Absolute or Differential Operation MSW
125		Module #7 Output 2 LSW Value
126		Module #7 Output 2 MSW Value (Pulse mode only)
127		Module #7 Output 2 Absolute or Differential Operation LSW
128		Module #7 Output 2 Absolute or Differential Operation MSW
129	Module #8 Input 1 Value Control Bit	Module #8 Input 1 LSW Value
130	Module #8 Input 2 Value Control Bit	Module #8 Input 1 MSW Value (Pulse mode only)
131		Module #8 Input 1 LSW Value Store (Pulse mode only)
132		Module #8 Input 1 MSW Value Store (Pulse mode only)
133		Module #8 Input 2 LSW Value
134		Module #8 Input 2 MSW Value (Pulse mode only)
135		Module #8 Input 2 LSW Value Store (Pulse mode only)
136		Module #8 Input 2 MSW Value Store (Pulse mode only)
137		Module #8 Output 1 LSW Value
138		Module #8 Output 1 MSW Value (Pulse mode only)
139		Module #8 Output 1 Absolute or Differential Operation LSW
140		Module #8 Output 1 Absolute or Differential Operation MSW
141		Module #8 Output 2 LSW Value
142		Module #8 Output 2 MSW Value (Pulse mode only)
143		Module #8 Output 1 Absolute or Differential Operation LSW
144		Module #8 Output 1 Absolute or Differential Operation MSW

5.4 Rotary Switches

On the top of each I/O module is an 8-position rotary switch. In the address maps Table 5-1 and Table 5-2 there are references to module numbers. These module numbers refer to the position of the rotary switch. Each module must have a different number.

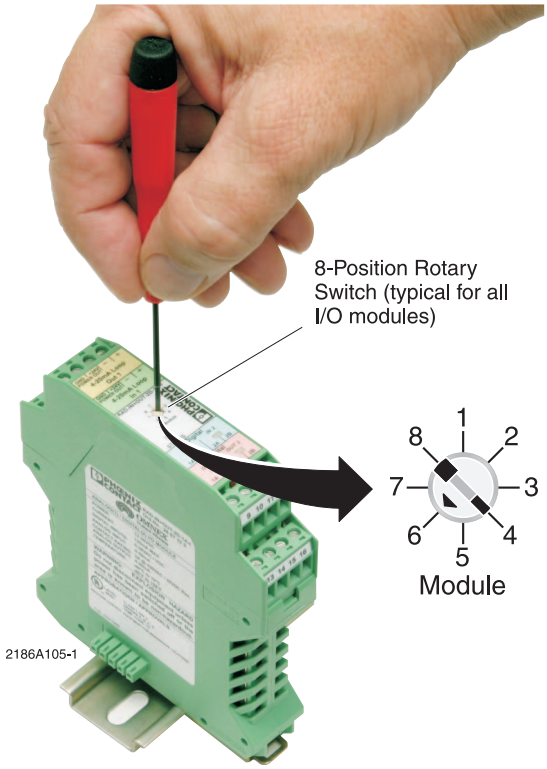


Figure 5-5 I/O module 8-position rotary switch

5.5 Register Scaling

5.5.1 Digital Channels

A digital output channel can be turned on by writing a “1” to the digital output register, and off by writing a “0” to the output register.

5.5.2 Analog Channel Scaling

Analog channels are scaled as follows:

$$\text{Current Input} = \frac{(\text{Register Value}) \bullet 22\ \text{mA}}{32767}$$

$$\text{Current Output} = \frac{(\text{X mA}) \bullet 32767}{22\ \text{mA}}$$

5.5.3 Pulse Input Channels

If the input channel is set to frequency mode, the value displayed in the corresponding register will be the input signal frequency in Hz (0-32 kHz).

If the pulse input channel is set to counter mode, each channel will have a 32-bit register (two consecutive 16-bit registers) assigned to it. The first (LSW) register keeps the current count (up to 32,767). To manually reset a channel to zero (0), simply write a “1” to the coil register that corresponds to that channel. Refer to the address map in this section to determine the correct register. A channel is reset to zero when the coil transitions from a “0” to a “1.”

NOTE:

If a pulse input channel set to counter mode, you may need to periodically reset the register to prevent overflow. To reset a channel to zero, simply write a “1” to the coil register that corresponds to that channel. Refer to the address map to determine which register. A reset command is executed when the coil transitions from a “0” to a “1.”

5.5.4 Pulse Output Channels

If the output channel is set to frequency mode, the value entered in the corresponding register will be the output signal frequency in Hz (0-32 kHz). In frequency mode, the only register that will respond to PLC commands is the least significant word (LSW). Because the most significant word (MSW) exceeds the maximum pulse frequency that the module can produce, any values written to it will be ignored.

If the pulse output channel is set to counter mode, each channel will have a 32-bit register (two consecutive 16-bit registers) assigned to it. The counter mode has two different types of operations: (1) absolute count; and (2) differential count. The two modes are described in the following paragraphs.

Absolute Mode

Pulses produced = New pulse count - Previous pulse count

In absolute mode, the total number of pulses provided is equal to the pulse output register value.

For example, if the previous value in the register was 5 and a new value of 15 is written, 10 pulses will be produced. However, if a new value of 3 were written, the pulse module would produce enough pulses to wrap the 32-bit register around until it is reset to 0 and then delivers 3 more pulses. Therefore, the pulse register should be cleared periodically.

Differential Mode

Pulses produced = New pulse count

In differential mode, the number of pulses produced is equal to each new value written to the pulse output register.

For example, if a value of 10 was written to the pulse output register, 10 pulses would be produced. If a new value of 5 were written, 5 more pulses would be produced.

To initialize absolute or differential counts, refer to the address map to determine which registers are used to control the operation mode. Absolute mode is initialized by writing 0 to both control registers; differential mode is specified by writing 1 to the LSW and 0 to the MSW.

Clearing A Counter Register

To clear a counter register when using Modbus RTU protocol, use function code 16 (multiple register write) and write a value of 0 (LSW), -32768 (MSW) to the pulse output counter.

NOTE:
When counter mode is selected, if the number of counts to be delivered is not completed before a new pulse count is written to the register, the new counts are added to the existing count.

NOTE:
(For OPC Servers)
If using an OPC server, it may not write the clear register values with a single instruction. Use differential mode if the OPC server commands cannot clear the counter. There is no need to clear counters in differential mode.

5.6 Wiring and Fail Condition DIP Switches for the I/O Modules

5.6.1 Analog Input Module

If using the Analog Input Module, use the wiring diagram shown in Figure 5-6.

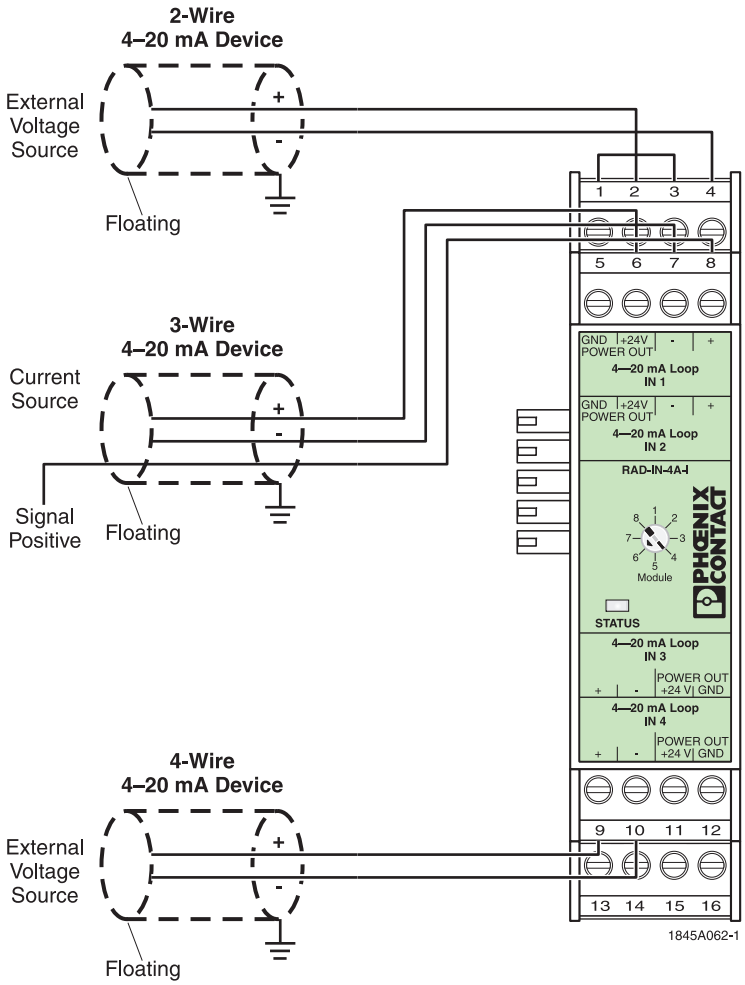


Figure 5-6 RAD-IN-4A-I Analog Input Module wire diagram

5.6.2 Digital Input Module

If using a Digital (Discrete) Input Module, use the wiring diagram shown in Figure 5-7.

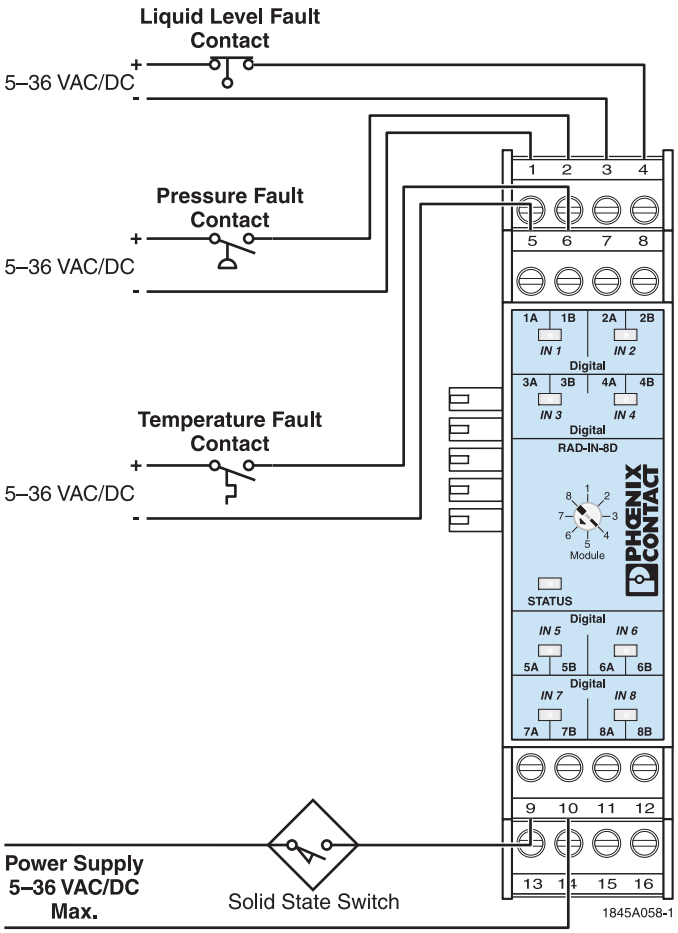


Figure 5-7 RAD-IN-8D Digital Input Module wire diagram

5.6.3 Analog Output Module

If using the Analog Output Module, use the wiring diagram shown in Figure 5-8.

Inside of the Analog Output Module are DIP switches that allow the user to determine the status of each channel if the RF link is lost. The options are Maintain Last State or Fault Off to a current value of approximately 2 mA. Release the top part of the housing to access the internal DIP switches.

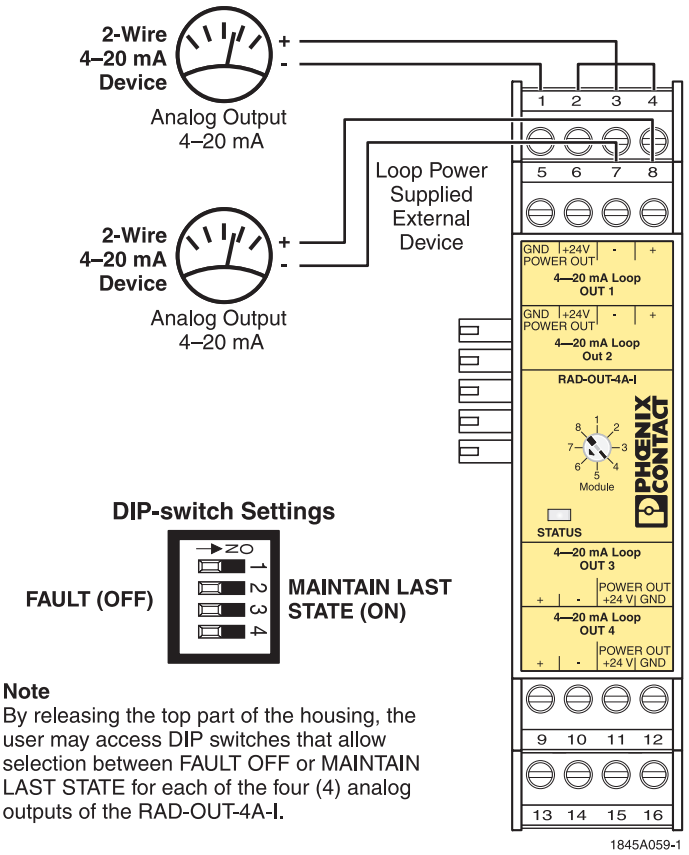


Figure 5-8 RAD-OUT-4A-I Analog Output Module wire diagram

5.6.4 Digital Output Module

If using the Digital Output Module, use the wiring diagram shown in Figure 5-9.

Inside of the Digital Output Module are DIP switches that allow the user to determine the status of each channel if the RF link is lost. The options are Maintain Last State or Fault Off (open circuit). Release the top part of the housing to access the internal DIP switches.

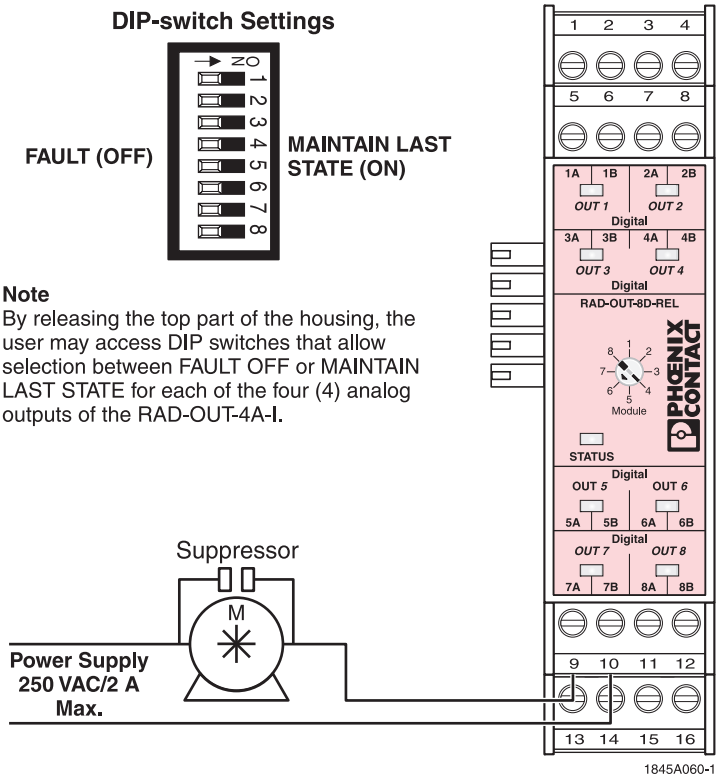


Figure 5-9 RAD-IN-OUT-8D-REL Digital Output Module wire diagram

5.6.5 Combination Input/Output Module

If using the Combo Module, use the wiring diagram shown in Figure 5-10.

Inside of the Combo Module are DIP switches that allow the user to determine the status of each channel if the RF link is lost. The options are Maintain Last State or Fault Off (open circuit). Release the top part of the housing to access the internal DIP switches.

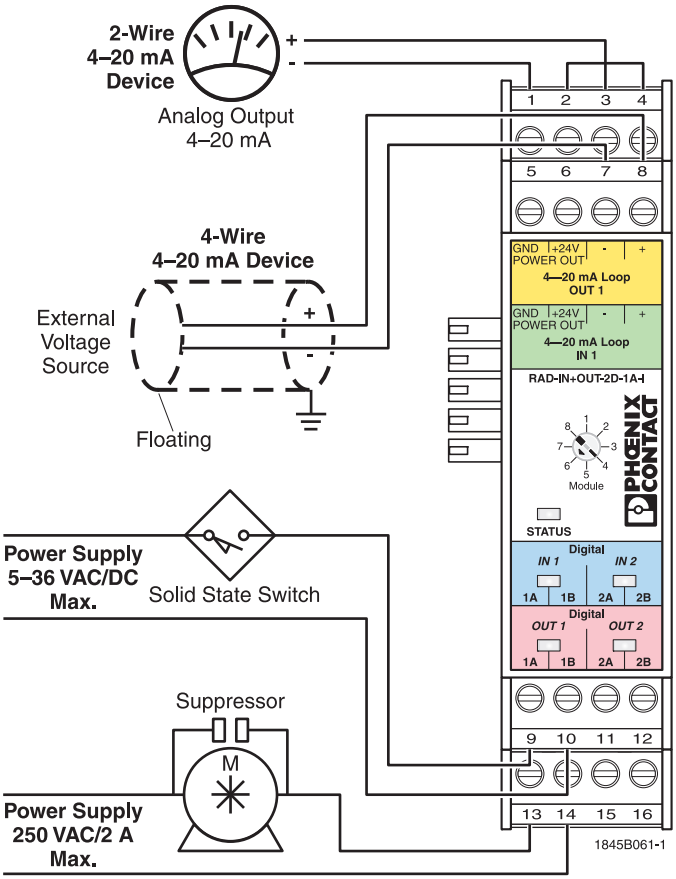


Figure 5-10 RAD-OUT-8D-REL Digital Output Module wire diagram

5.6.6 Digital Pulse Input Module

The Digital Pulse Input Module accepts pulse signals from many different types of devices.

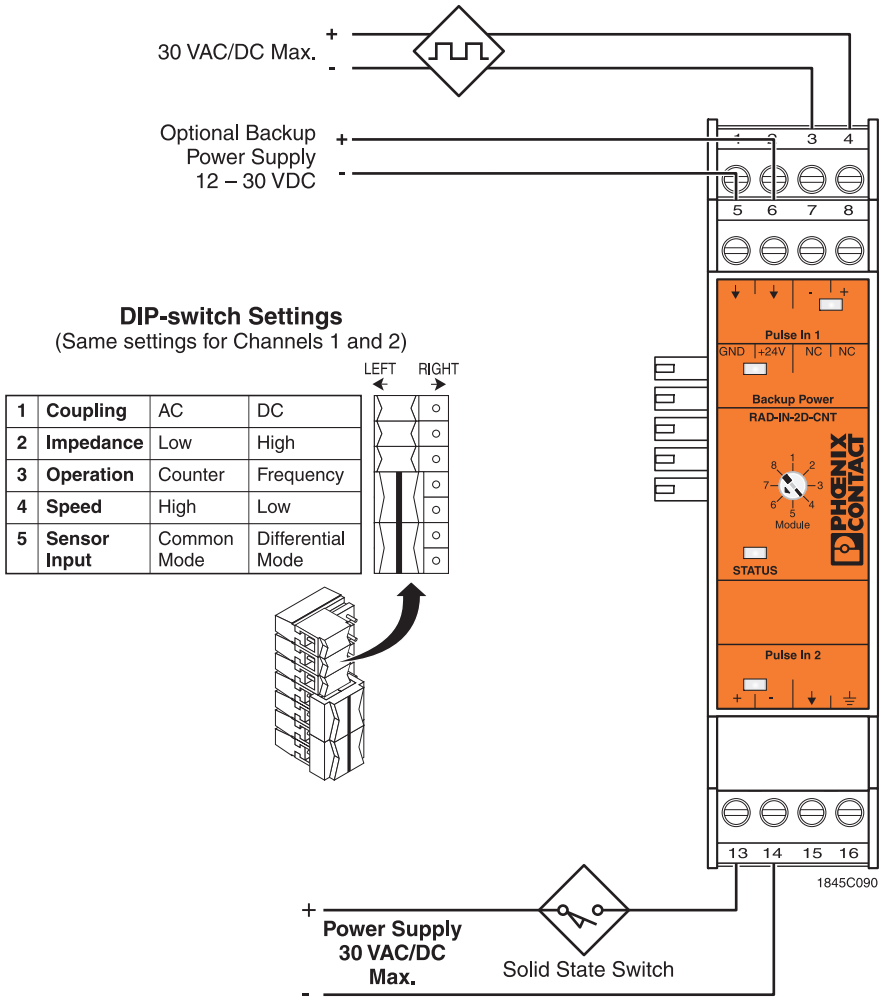


Figure 5-11 RAD-IN-2D-CNT Pulse Input Module wire diagram

Backup Power

The Digital Pulse Input Module will retain its pulse count if power is removed; however, it will not record any new pulses. Terminals 5 and 6 are used for connecting the backup power supply to the module. If primary power (through the bus connector from the radio) is lost, the backup power supply allows the module to continue to record pulses. The backup power terminals will not supply power to the transceiver or any other module on the bus connector.

DIP Switch Settings

Refer to Figure 5-10 on page 5-22 for DIP switch configurations.

AC/DC Coupling

Set the jumper to AC Coupling if the pulse voltage will never drop below 3.6 V with respect to the transceiver's power supply negative. This would apply where there is a DC bias voltage added to the pulse input voltage, where the DC bias exceeds 3.6 V such as in a ground loop condition. All other applications, including an AC sine wave input, should be set to DC Coupling.

Low/High Input Impedance

The low impedance setting has input impedance of 1 kΩ, and the high setting has impedance of 90 kΩ. High impedance should be used with magnetic transducers to prevent the current draw from dropping the voltage below the 100 mV AC peak-to-peak minimum. The low impedance setting should be used with digital and relay interfaces because the additional current draw will prevent electrical noise from causing false pulse counts.

Counter/Frequency Operating Mode

The pulse input values can be stored in the PLC register in two formats; either a count of the number of pulses or a frequency value. The frequency setting will take the average number of pulses every second.

Low/High Speed Operation

The low speed pulse setting is restricted to a maximum input frequency of 2 Hz with a minimum pulse width of 70 ms. The high speed setting is designed for pulse frequencies up to 32 kHz and requires a 10 µs minimum pulse width. Use the low speed setting for mechanical pulse generating devices such as relays and the high speed setting for all other applications. The low speed setting prevents contact bounce from being recorded as pulses.

Single Ended/Differential Input

If the pulse signal is expected to be of negative polarity, with respect to ground, set the module to differential input. If the signal is to remain positive at all times, set it to single ended.

Diagnostic LEDs

There are four diagnostic LEDs on the Digital Pulse Input Module. See Figure 5-12 for the meaning of each LED.

LED Name	State	Meaning
Status	ON solid	I/O is functional
	Flashing	Conflict with another module
Backup Power	OFF	Primary power is powering the module
	ON solid	Backup power supply is powering the module
Pulse Input 1 & 2		
Pulse Frequency (Hz)	Flashing (Hz)	LED will flash at various rates based on the pulse applied to each channel
1 to 10 Hz	1	
11 to 100 Hz	5	
101 to 1000 Hz	8	
1001 to 32K	ON solid	

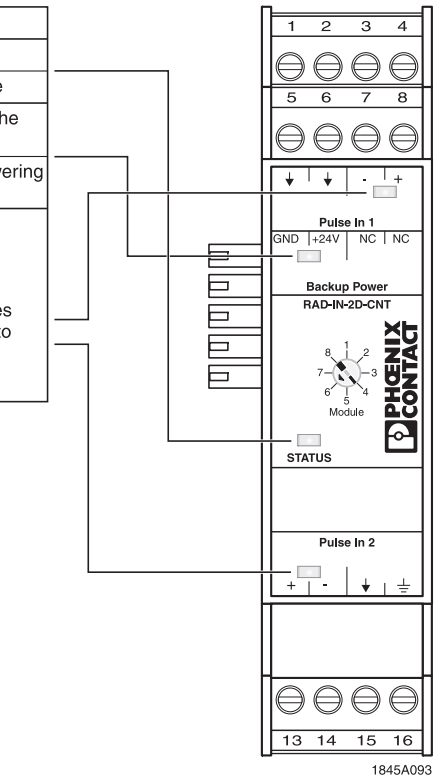
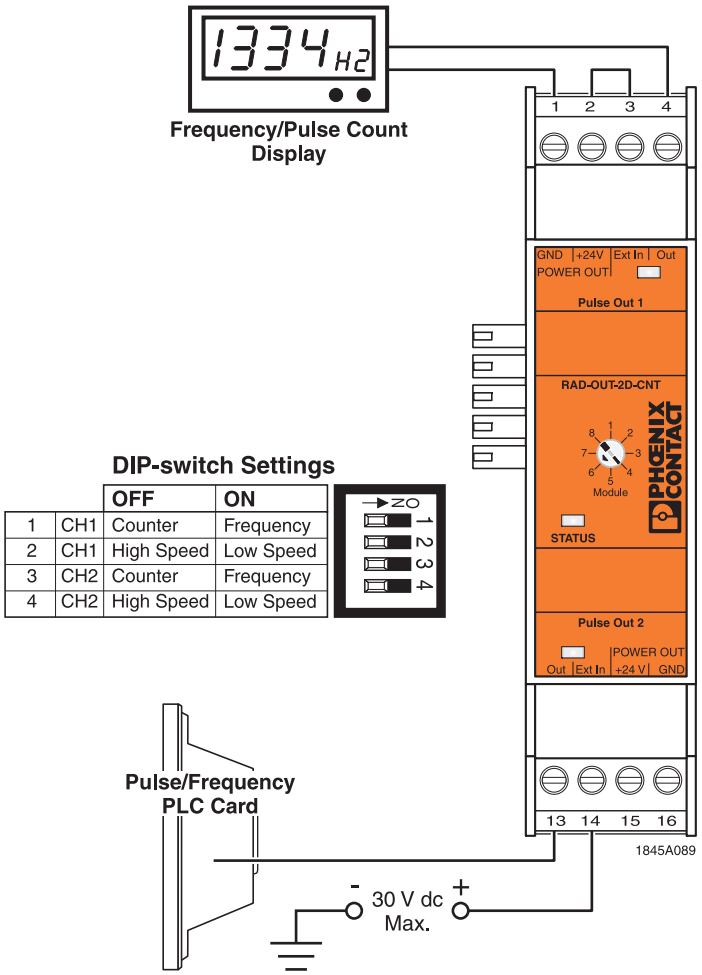


Figure 5-12 Description of RAD-IN-2CNT Digital Pulse Input Module LEDs

5.6.7 Digital Pulse Output Module

The Digital Pulse Output Module accurately reproduces pulse counts or frequency outputs from data contained in PLC registers. It is compatible with mechanical relays and electronic pulse input devices. Upon power loss, the pulse output is set to 0 Hz.



		OFF	ON
1	CH1	Counter	Frequency
2	CH1	High Speed	Low Speed
3	CH2	Counter	Frequency
4	CH2	High Speed	Low Speed

Figure 5-13 RAD-OUT-2D-CNT Digital Pulse Output Module wire diagram

DIP Switch Settings

The DIP switch settings listed below are applicable for both channel 1 and channel 2. Refer to Figure 5-13 for DIP switch configurations.

Counter/Frequency Mode

When counter mode is selected, the module will output a specific number of pulses as determined by the PLC value written to it. If frequency mode is selected, the pulse output module will generate pulses with a 50% duty cycle. In frequency mode, the low or high speed switch setting is ignored.

Low/High Speed Operation

This switch setting only impacts counter mode. If high speed is selected, the pulses will be sent at a frequency of 10 kHz with a 50% duty cycle. If low speed is selected, the pulses will be sent at a frequency of 10 Hz also with a 50% duty cycle.

Diagnostic LEDs

There are three diagnostic LEDs on the Digital Pulse Output Module. See Figure 5-14 for the meaning of each LED.

LED Name	State	Meaning
Status	ON solid	I/O is functional
	Flashing	Conflict with another module
Pulse Input 1 & 2		
Pulse Frequency (Hz)	Flashing (Hz)	
1 to 10 Hz	1	LED will flash at various rates based on the pulse applied to each channel
11 to 100 Hz	5	
101 to 1000 Hz	8	
1001 to 32K	ON solid	

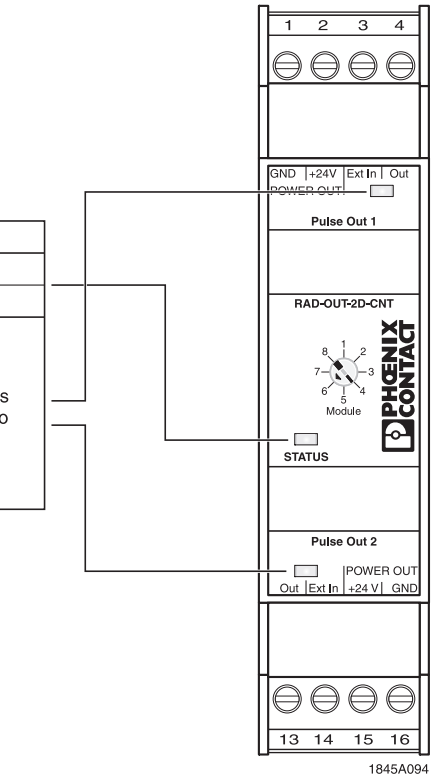


Figure 5-14 Description of RAD-OUT-2D-CNT Digital Pulse Output Module LEDs

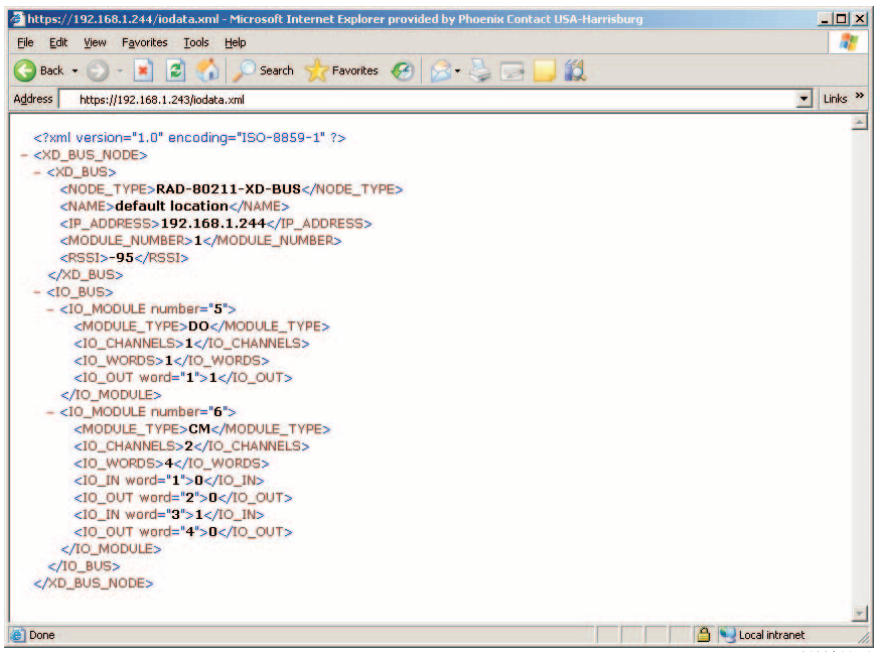
5.7 Accessing the XML file

To access the read-only XML file containing the status of the I/O modules, do the following:

1. Open a web browser and enter the IP address of the RAD-80211-XD-BUS with connected I/O modules.
2. Log onto the radio using the appropriate password. Then click the link on the left-hand menu to view the file. To access the file using a custom program such as a Microsoft Excel spreadsheet, enter the IP address of the radio to be accessed in the following format:

   https://aaa.bbb.ccc.ddd/iodata.xml

Figure 5-15 is an example of how the data is displayed for two I/O modules with rotary switch settings 5 and 6:



2186A115-1

Figure 5-15 Example of data display

Section 6

This section informs you about
- LED indicators
- RSSI
- General troubleshooting
- Resetting the IP address

Radio Troubleshooting 6-3

6.1 LED Indicators 6-3
6.1.1 RAD-80211-XD and RAD-80211-XD-BUS 6-3
6.1.2 RAD-80211-XD-WM 6-4

6.2 RSSI (Received Signal Strength Indicator) 6-5
6.2.1 RAD-80211-XD and RAD-80211-XD-BUS 6-5
6.2.2 RAD-80211-XD-WM 6-6

6.3 General Troubleshooting 6-7

6.4 Resetting the IP Address 6-9
6.4.1 DOS Command 6-9
6.4.2 Hardware Reset 6-9

6 Radio Troubleshooting

6.1 LED Indicators

6.1.1 RAD-80211-XD and RAD-80211-XD-BUS

Figure 6-1 defines the LED indicator meanings for the RAD-80211-XD and RAD-80211-XD-BUS Radios. Figure 6-2 defines the LED indicator meanings for the RAD-80211-XD-WM.

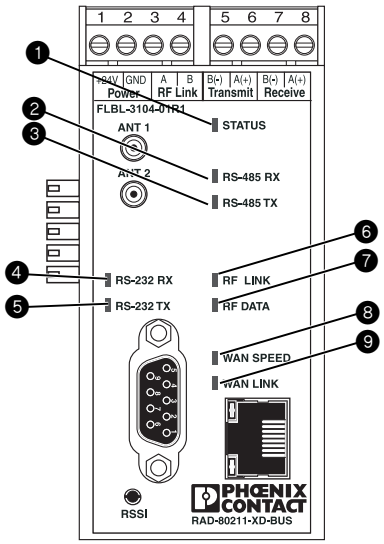


Figure 6-1 RAD-80211-XD and RAD-80211-XD-BUS LED locations

Table 6-1 LED descriptions

No.	LED Name	LED Color	LED Status	Description
1	Status	Green	On	Normal operation
			Flashing slowly	Internal error
			Flashing fast	Application error[1]
2	RS-485RX	Green	Flashing	RS-422/485 data is being transmitted
3	RS-485TX	Green	Flashing	RS-422/485 data is being received
4	RS-232RX	Green	Flashing	RS-232 data is being transmitted
5	RS-232RX	Green	Flashing	RS-232 data is being received
6	RF Link	Green	On	RF link is established
7	RF Data	Green	Flashing	Data is being transmitted/received
8	WAN Speed	Green	On	100Base-T connection
9	WAN Link	Green	Flashing	Data is detected on Ethernet port

[1] Typical application error is a Modbus I/O timeout

6.1.2 RAD-80211-XD-WM

Figure 6-2 defines the LED indicator meanings for the RAD-80211-XD-WM. These LEDs can assist in troubleshooting the radio.

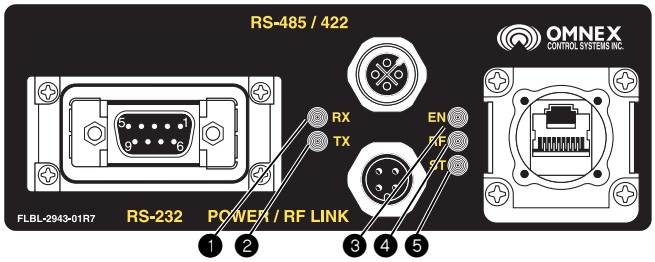


Figure 6-2 RAD-80211-XD-WM LED locations

Table 6-2 LED descriptions

No.	LED Name	LED Color	LED Status	Description
1	TX	Green	Flashing	RS-232 data is being transmitted
2	RX	Green	Flashing	RS-232 data is being received
3	EN	Green	On	Wired network is connected
4	RF	Green	On	Transceiver has valid RF link with another transceiver
5	ST	Green	Flashing	Internal error has occurred

6.2 RSSI (Received Signal Strength Indicator)

The RSSI test point allows measurement of the received radio signal strength at each client or bridge (see Figure 6-3). RSSI will not function on an access point because there is no method of determining which client is connected. The RSSI is a voltage output, ranging from 0-3.5 V DC, and can be measured using a standard voltmeter.

6.2.1 RAD-80211-XD and RAD-80211-XD-BUS

On models RAD-80211-XD and RAD-80211-XD-BUS, the positive connection for the multimeter is made on the RSSI test point of the radio and the negative connection to the power supply ground. An adapter is available that will connect to the RSSI connector to allow permanent monitoring of the RSSI voltage (Order No. 0201744 for test connector and Order No. 0201663 for insulating sleeve).

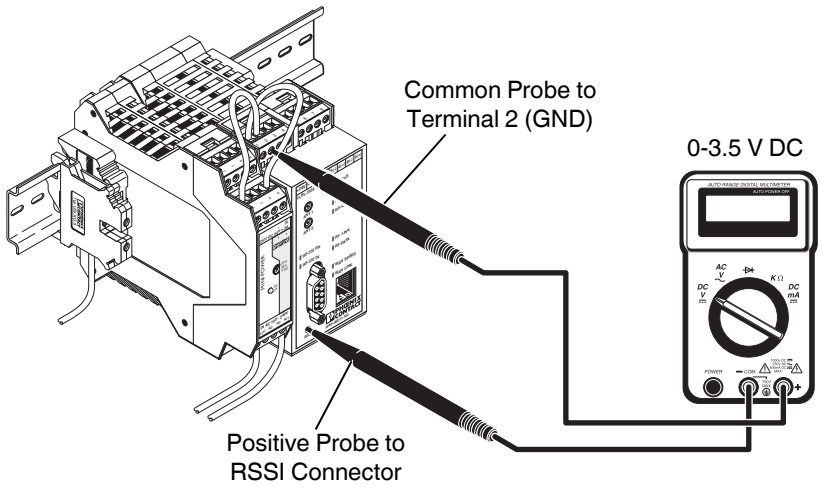


Figure 6-3 RAD-80211-XD and RAD-80211-XD-BUS RSSI voltage strength check

6.2.2 RAD-80211-XD-WM

On model RAD-80211-XD-WM, the positive connection is made on the RSSI test point and the negative lead is connected to the bolt under the antenna on the right side of the unit. See Figure 6-4.

The voltage measured directly correlates to the received signal expressed as -dBm. Note that this voltage will fluctuate constantly due to multipathing.

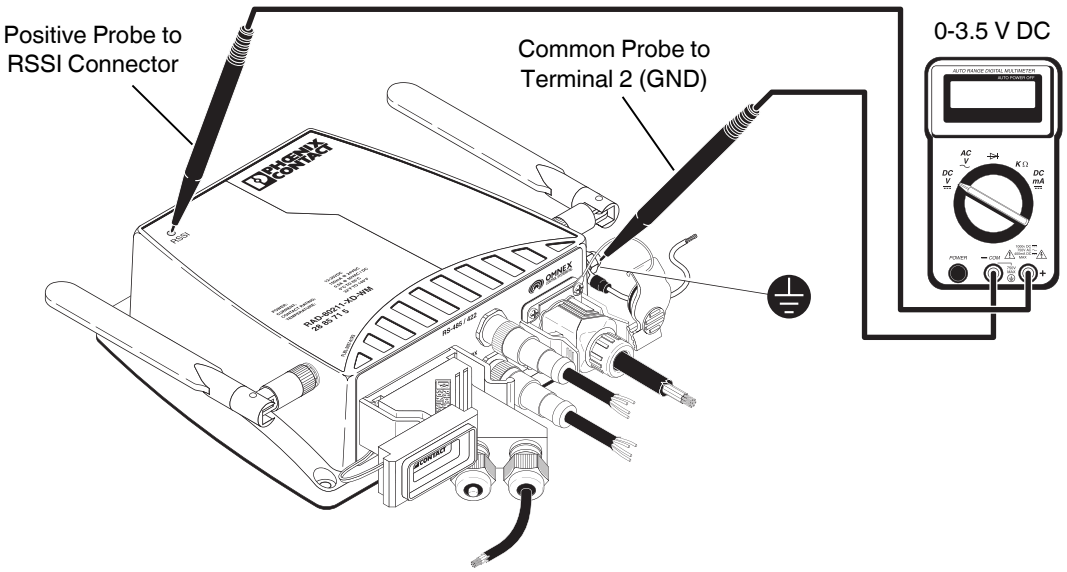


Figure 6-4 RAD-80211-XD-WM RSSI voltage strength check

Measuring the RSSI voltage provides a simple way to align antennas. This is very useful with longer distance communication systems where directional antennas are positioned using a simple volt meter and adjusting the antennas based on change of signal strength

(see Figure 6-5). The RSSI voltage can also be used to estimate an expected data transfer speed of the radio network. Using the RSSI voltage, the power can be determined in dBm. The dBm value converts to a data throughput value using Table 6-3.

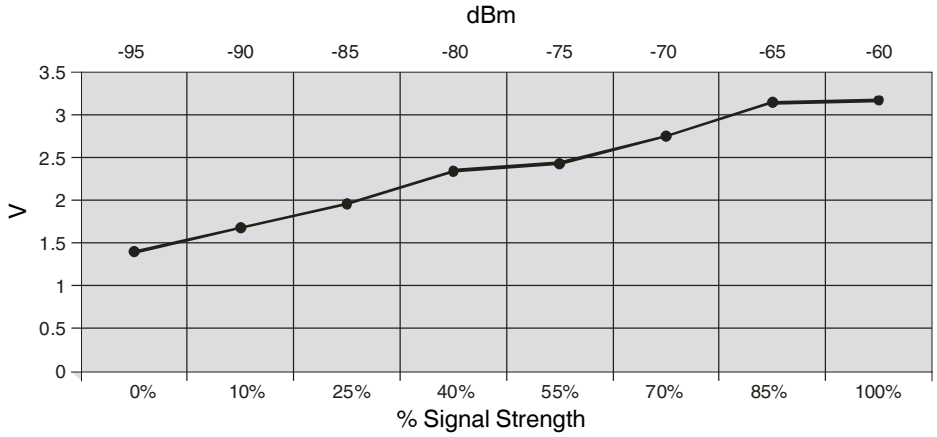


Figure 6-5 Voltage vs. Signal Strength

Table 6-3 Expected Raw Data Throughput

802.11a		802.11b		802.11g	
Mbps	**dBm**	**Mbps**	**dBm**	**Mbps**	**dBm**
54	-71	11	-90	54	-74
48	-73	5.5	-92	48	-76
36	-76	2	-94	36	-79
24	-78	1	-95	24	-81
18	-81			18	-83
12	-83			12	-85
9	-85			9	-87
6	-88			6	-90

6.3 General Troubleshooting

When troubleshooting a network, the first step is to ensure there is a good radio signal. Once that has been established, check the wiring between the radio and external devices. After the wiring has been verified, then you can adjust configuration parameters.

The most practical method of troubleshooting a system is to lay all of the components out on a table, such that all radios are within 3 m (10 ft.) of each other. This way there will be a strong radio signal, and programming each radio will not involve traveling to a remote site.

Refer to Table 6-4 to help identify various problems and possible solutions.

Table 6-4 RAD-80211-XD... Troubleshooting Procedures

Problem	Solution
Unable to open Web-Based Management	1. Ensure power is applied to radio. 2. Ensure cable is connected between PC and radio (WAN LINK LED will be on if cable is connected). 3. Verify network settings of PC match network settings of radio. 4. The LAN Link and Duplex selection in the radio should match the settings of the connected wired network. Select Auto if in doubt. 5. Confirm IP address of radio. If IP address is unknown, it can be set using a DOS command. See “Resetting the IP Address” in this section.
No radio link (radios within 10 feet of each other) [Access Point/Client Modes]	1. Ensure one radio is programmed as an Access Point and the others as clients. 2. Verify selected wireless modes are compatible (802.11a or 802.11b/g). 3. Confirm security settings match in each radio.
No radio link (radios within 10 feet of each other) [Bridge Mode]	1. Ensure BSSID of remote radio is entered in local radio and vice versa. 2. Verify selected wireless modes are compatible (802.11a or 802.11b/g) and wireless channels match in each radio. 3. Confirm security settings match in each radio.
No radio link (field installed)	1. Check to ensure antennas are connected and aimed properly. 2. Inspect antenna connections; they should be tight and corrosion free. 3. Increase the mounting height of the antenna to gain line-of-sight. 4. Install larger gain antenna (and/or decrease coaxial cable loss). 5. Use a Wi-Fi scanner to check for nearby networks that may cause interference. 6. Check the power supply to ensure sufficient current capacity. 7. Make sure the center pin of the antenna coaxial cable is not shorted to ground.
Able to send data, but no response from remote device	1. Verify network settings in remote device match those of the radios and LAN. – Each device should have a unique IP address in the same network (e.g. 192.168.254.xxx). – The Subnet Mask should be the same in each device. – The LAN Link and Duplex selection in the radio should match the settings of the connected wired network. Select Auto if in doubt.

6.4 Resetting the IP Address

If the IP address is unknown, access to the radio can be restored by changing the IP address using either a DOS command or a hardware reset.

6.4.1 DOS Command

Open a DOS prompt in Windows by clicking Start, Run, and typing “cmd” without quotes. A C:/ prompt will open. At the prompt, do the following steps.

1. Enter arp -s (desired IP address) (MAC address of radio).
   – For example: arp -s 192.168.254.200 00-aa-00-62-c6-09
2. Hit Enter. Then type: ping -l 1040 (IP address)
   – For example: ping -l 192.168.254.200

NOTE:
The character in “ping-l” is a lower case “L.” If the IP address assignment was successful, a reply message will appear. To abort the ping, press Ctrl+C.

6.4.2 Hardware Reset

The hardware reset will restore the default IP address 192.168.254.254 as well as the default user passwords “admin” for the Admin user and “monitor” for the monitor user. To initiate a hardware reset, disconnect power from the radio and insert a jumper across pins 2 and 3 on the DB-9 RS-232 port. Reconnect power. Once startup is complete, remove the jumper.

Section 7

This section informs you about
– Dimensions and specifications

Technical Data 7-3

7.1 RAD-80211-XD and RAD-80211-XD-BUS 7-3

7.2 RAD-80211-XD-WM 7-4

7.3 Dimensions 7-5

7 Technical Data

7.1 RAD-80211-XD and RAD-80211-XD-BUS

Wireless Data	
Frequency	
802.11b/g	2.4-2.4835 GHz
802.11a	5.25-5.815 GHz
Transmit power	100 mW maximum (adjustable to 1 mW)
Channel selection	
802.11b/g	1-11
802.11a	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

General Data	
Power	12 to 30 V DC
Wiring connections	
Power port	screw terminal 12 to 24 AWG
RS-232 port	DB-9 female
RS-422/485 port	screw terminal 12 to 24 AWG
Ethernet port	RJ45
Mounting	NS35 DIN rail
Dimensions (LxWxH)	99 x 45 x 115 mm (3.90 x 0.88 x 4.5 in.)
Case material	plastic
Temperature range	0 to 65°C (32 to 149°F)
Degree of protection	IP20
LED Indicators	
Power	ON solid when 12 to 30 V DC is applied
RS-485TX	flashes when RS-422/485 data is transmitted
RS-485RX	flashes when RS-422/485 data is received
RS-232TX	flashes when RS-232 data is transmitted
RS-232RX	flashes when RS-232 data is received
RF Data	flashes when data is sent/received
RF Link	ON solid when RF link is established
WAN Link	flashes when data is detected on Ethernet port
WAN SPEED	ON solid when 100 Base-T connection exists
WAN SPEED	OFF when no 100 Base-T connection exists
Antenna connector	MCX female (2x)

Approvals/Conformance	
FCC ID (USA)	NKRCM9
UL	Class I, Div. 2, Groups A, B, C, and D Wi-Fi® compliant

7.2 RAD-80211-XD-WM

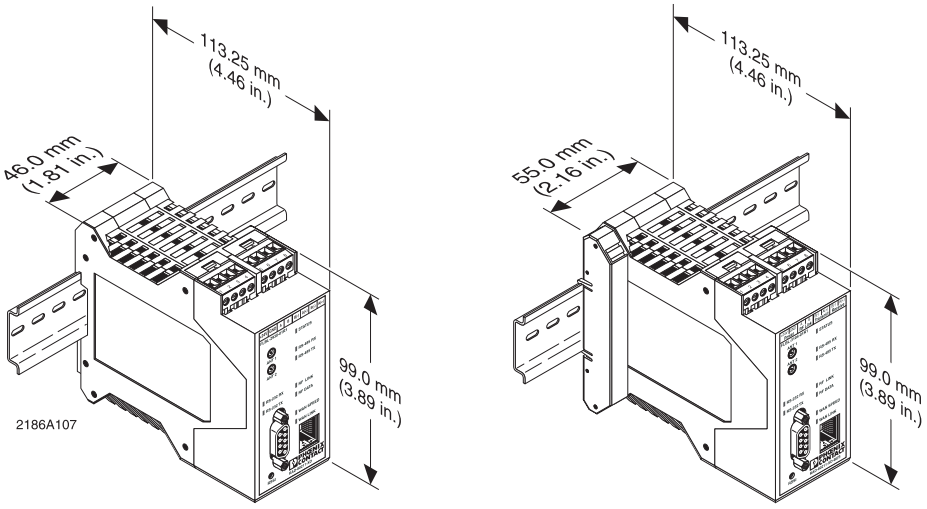
Wireless Data	
Frequency	
802.11b/g	2.4-2.4835 GHz
802.11a	5.25-5.815 GHz
Transmit power	100 mW maximum (adjustable to 1 mW)
Channel selection	
802.11b/g	1-11
802.11a	52,56,60,64,149,153,157,161

General Data	
Power	Power-over-Ethernet (PoE) or 12 to 30 V DC
Wiring connections	
Power	M12
RF Link Contact	M12
RS-232 port	IP54 DB-9 female
RS-422/485 port	M12
Ethernet port	IP54 RJ45 VARIOSUB
Mounting	wall mount
Dimensions (LxWxH)	178 x 165 mm (7.00 x 6.49 in.)
Case material	Xenoy 522OU plastic
Temperature range	0 to 65°C (32 to 149°F)
Degree of protection	IP54
Approvals	UL Class I, Div 2, Groups A, B, C, and D; Wi-Fi compliant
LED indicators	
TX	flashes when RS-232 data is transmitted
RX	flashes when RS-232 data is received
ST	ON when WLAN is operating normally
ST	flashes to indicate internal errors
RF	ON solid when RF link is established
EN	ON solid when 100 Base-T connection exists
EN	OFF when no 100 Base-T connection exists
Antenna connector	RPSMA female (2x)

Approvals/Conformance	
FCC ID (USA)	NKRCM9
UL	Class I, Div 2, Groups A, B, C, and D Wi-Fi compliant

7.3 Dimensions

Figure 7-2 and Figure 7-1 provide the basic dimensions of the RAD-80211-XD, RAD-80211-XD-BUS and RAD-80211-XD-WM transceivers.



RAD-80211-XD Transceiver **RAD-80211-XD-BUS Transceiver**

Figure 7-1 RAD-80211-XD and RAD-80211-XD-BUS Transceiver Dimensions

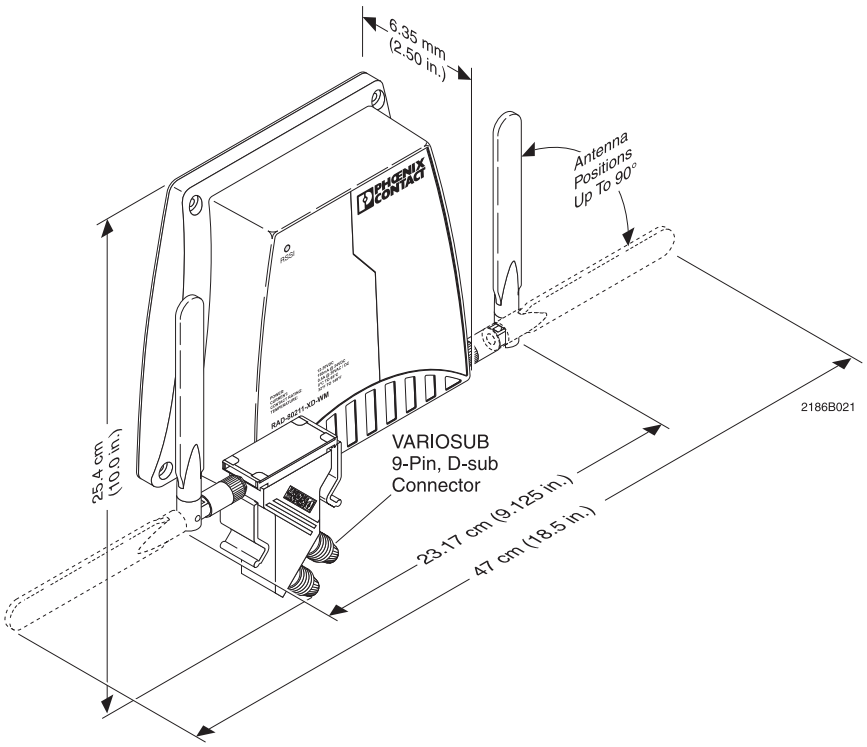


Figure 7-2 RAD-80211-XD-WM Transceiver Dimensions

Section 8

This section informs you about

– Ordering information for parts, assemblies, and accessories

Ordering Information 8-3

8.1 RAD-80211-XD and RAD-80211-XD-BUS Parts and Assemblies 8-3

8.2 RAD-80211-XD-WM Parts and Assemblies 8-5

8.3 Additional Parts and Accessories 8-6

8 Ordering Information

8.1 RAD-80211-XD and RAD-80211-XD-BUS Parts and Assemblies

Figure 8-1 shows the various parts and assemblies applicable to the RAD-80211-XD and RAD-80211-XD-BUS radios. Table 9-1 lists the part number and description for each item identified in Figure 8-1.

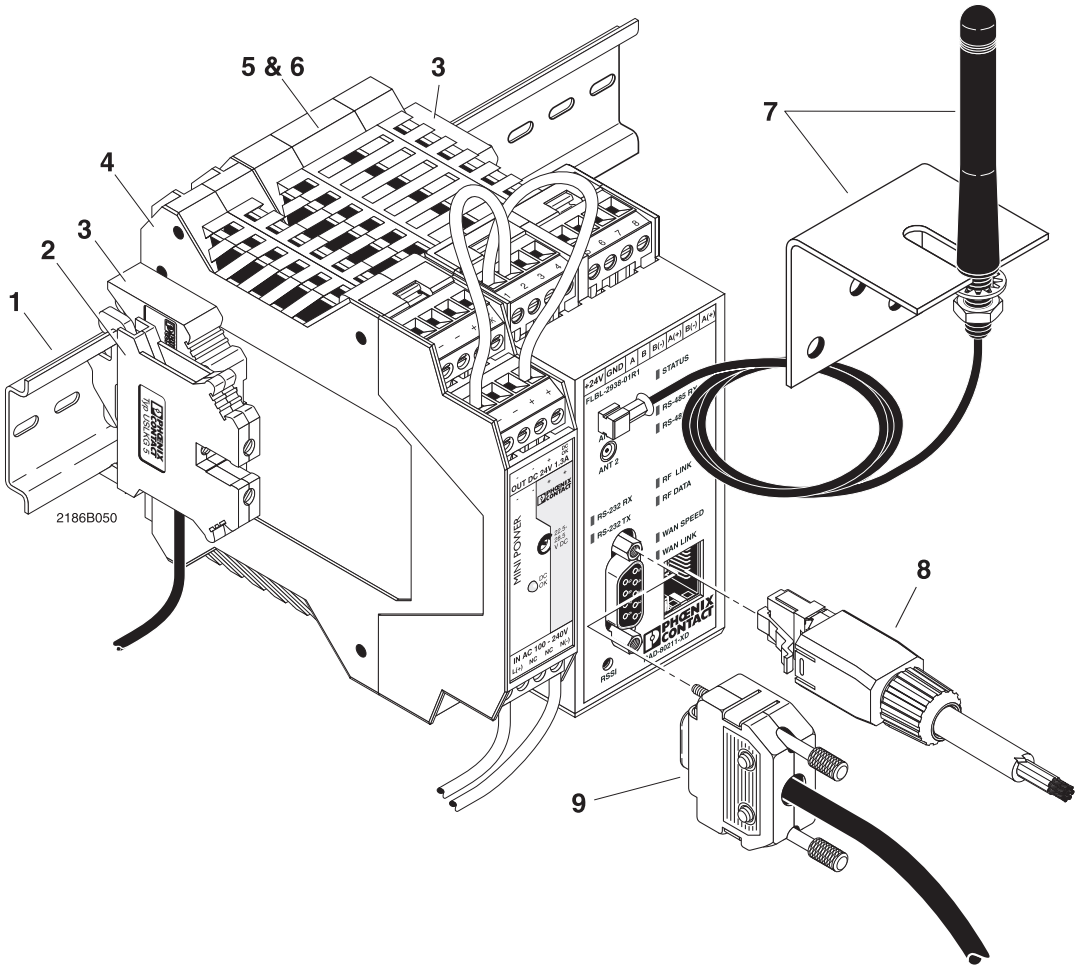


Figure 8-1 Parts and Assemblies for the RAD-80211-XD and RAD-80211-XD-BUS Radio

Table 8-1 RAD-80211-XD and RAD-80211-XD-BUS Part Listing

Item No.	Description	Type	Order No.
1	DIN rail, 35 x 7.5 mm, perforated, 2 m (6/56 ft.) long	NS 35/65 GELOCHT	0801733
2	Universal ground terminal block	USLKG5	0441504
3	Universal end bracket for NS35 DIN rail	E/NS 35 N	0800886
4	MINI power supply, 100-240 V AC input, 24 V DC output, 1.3 A	MINI-PS-100-240AC/24DC/1.3	2866446
5	802.11 a/b/g industrial radio transceiver, DIN rail mount	RAD-80211-XD	2885728
6	802.11 a/b/g industrial radio transceiver, DIN rail mount	RAD-80211-XD-BUS	2885757
7	2 dBi gain omnidirectional antenna, IP65 protection, with bracket and 1.5 m (4.92 ft.) long adapter cable	RAD-ISM-2400-ANT-OMNI-2-1	2867461
8	Ethernet cable assembly (purple), 8-position, one end RJ45 (1P67), one end RJ45 (IP20), 5 m (16.40 ft.) long	VS-08-LI-VSIP67-VSIP20-CF-5,0	1689598
9	D-Sub cable assembly, 9-position, one male end & one female end, 3.0 m (9.85 ft.) long	CABLE-D 9SUB/B/S/300KONFEK/S	2302023

8.2 RAD-80211-XD-WM Parts and Assemblies

Figure 8-2 shows the various parts and assemblies applicable to the RAD-80211-XD-WM radio. Table 8-2 lists the part number and description for each item identified in Figure 8-2.

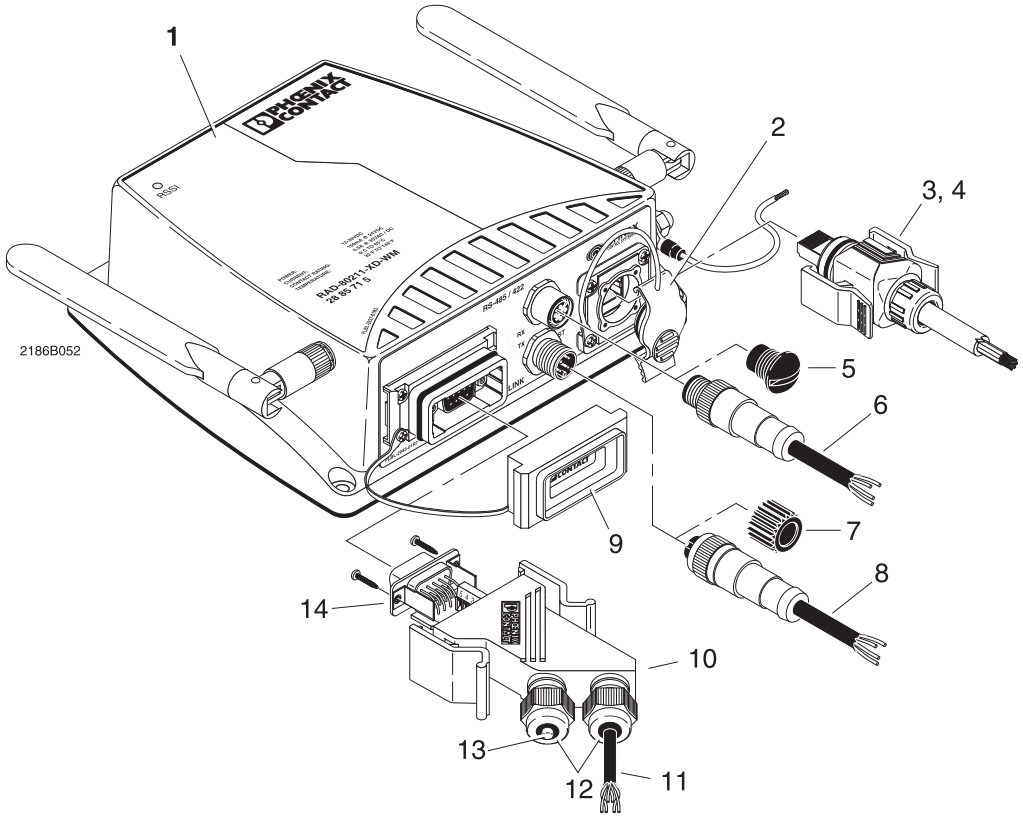


Figure 8-2 Parts and Assemblies for the RAD-80211-XD-WM Radio

Table 8-2 RAD-80211-XD-WM Part Listing

Item No.	Description	Type	Order No.
1	802.11 a/b/g industrial radio transceiver, wall mount	RAD-80211-XD-WM	2885715
2	Protective cover, RJ45 port	VS-08-SD-F	1652606
3	Connector, RJ45 (IP67), includes hood and connector	VS-08-T-RJ45/IP67-SET	1689475
4[1]	Ethernet patch cable, purple, CAT5, 4-pair shielded, connection not crossed (line), one end RJ45 (IP67), one end RJ45 (IP20), 5 m (16.4 ft.) long	VS-08-4X2X26C6/7-VS67-RJ45/5,0	1653207
5	Protective cap, M12 port, for unused position	PROT-M12	1680539
6[1]	Sensor/actuator cable assembly, one end has 4-position, male M12 straight plug, other end has free wires, 1.5 m (4.92 ft.) long	SAC-4P-M12MS/1,5-PUR	1668043
7	Protective cap, M12 port, for unused position	PROT-M12-M	2736194

Table 8-2 RAD-80211-XD-WM Part Listing

Item No.	Description	Type	Order No.
8[1]	Sensor/actuator cable assembly, one end has 4-position, female M12 straight socket, other end has free wires, 1.5 m (4.92 ft.) long	SAC-4P-1,5-PUR/M12FS	1668108
9	Protective cover, RS-232 port	VS-09-SD	1887086
10	RS-232 D-Sub hood (IP67)	VS-09-T-2M16	1688353
11[2]	Cable, 3 twisted pairs, shielded, highly flexible, sold by the meter	IBS RBC METER-T	2806286
12	Cable gland for D-Sub hood, accepts cable diameters from 3 to 6 mm	VS-M16 (3-6)	1688450
13	Cable gland sealing cap, for unused sealing positions	Q-PROT-9/11	1670235
14[3]	VARIOSUB D-sub insert, male, 9-position, 0.5 mm screw-clamp connection	VS-09-ST-DSUB/9-MPT-0,5	1688379

1 Other lengths are available upon request.

2 For 8- or 10-conductor cables, see your local distributor.

3 VARIOSUB D-sub inserts are available for different field busses or applications. They are also available in both screw-clamp and spring-clamp termination methods.

8.3 Additional Parts and Accessories

Table 9-3 lists parts and accessories that are available for use with the RAD-80211-XD, RAD-80211-XD-BUS and RAD-80211-XD-WM radios. You can find more products, accessories, guides, system configurators, etc. for wireless solutions by visiting our web site at:

www.phoenixcontact.com

Table 8-3 Accessories

Item No.	Description	Type	Order No.
1	8 dBi gain directional antenna, IP65 protection, connection type SMA (female), for 802.11b/g	RAD-ISM-2400-ANT-PAN-8-0	2867610
2	9 dBi gain omnidirectional antenna, IP65 protection, connection type N (female), for 802.11a	RAD-ISM-2400-ANT-OMNI-9-0	2867623
3	24 dBi gain directional parabolic dish and mounting bracket, connection type N (female), for 802.11a	RAD-ISM-2400-ANT-PARI-22-N	5606174
4	RG213 cable, 7.62 m (25 ft.) long, connection type N (male)	RAD-CAB-RG213-25	2867597
5	Surge protector for 2.4 GHz to 5.8 GHz antennas, connection type N (female) to N (female)	CN-LAMBDA/4-5.9-BB	2838490
6	Adapter, MCX (male) to N (male), for connection to radio and surge protector, 1.2 m (4 ft.) long	RAD-CON-MCX90-N-SS	2885207

A Technical Appendix

A 1 Structure of IP Addresses

A 1.1 Valid IP Parameters

IP parameters comprise the following three elements: “IP address,” “subnet mask,” and “default gateway/router.”
000.000.000.001 to 126.255.255.255 and
128.000.000.000 to 223.255.255.255

A 1.2 Valid Subnet Masks are:

255.000.000.000 to 255.255.255.252

A 1.3 Default Gateway/Router:

The IP address of the gateway/router must be in the same subnetwork as the address of the switch.

A 2 Assigning IP Addresses

The IP address is a 32-bit address. See Figure A-1. The IP address consists of a network part and a user part. The network part consists of the network class and the network address. There are currently five defined network classes. See Table A-1. Classes A, B, and C are used in modern applications, while classes D and E are hardly ever used. It is therefore usually sufficient if a network device only “recognizes” classes A, B, and C.

Figure A-1 Location of Bits within the IP Address

With binary representation of the IP address, the network class is represented by the first bits. The key factor is the number of “ones” before the first “zero.” The assignment of classes is shown in Table A-1. The empty cells in the table are not relevant to the network class and are already used for the network address.

Table A-1 Class Assignments

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Class A	0				
Class B	1	0			
Class C	1	1	0		
Class D	1	1	1	0	
Class E	1	1	1	1	0

The bits for the network class are followed by those for the network address and user address. Depending on the network class, a different number of bits are available, both for the network address (network ID) and the user address (host ID). See Table A-2.

Table A-2 Network and User Class Bit Assignments

	Network ID	Host ID
Class A	7 Bits	
Class B	14 Bits	
Class C	21 Bits	
Class D	28-Bit Multicast Identifier	
Class E	27 Bits (Reserved)	

IP addresses can be represented in decimal or hexadecimal form. In decimal form, bytes are separated by dots (dotted decimal notation) to show the logical grouping of the individual bytes. See Figure A-2.

NOTE:

The decimal points do not divide the address into a network and user address. Only the value of the first bits (before the first “zero”) specifies the network class and the number of remaining bits in the address.

Figure A-2 Structure of IP Addresses

A 2.1 Special IP Addresses for Special Applications

Certain IP addresses are reserved for special functions. The following addresses should not be used as standard IP addresses.

127.x.x.x Addresses

The class A network address “127” is reserved for a loopback function on all PCs, regardless of the network class. This loopback function may only be used on networked PCs for internal test purposes.

If a telegram is addressed to a PC with the value 127 in the first byte, the receiver immediately sends the telegram back to the transmitter. In this way, it is possible to check, for example, whether the TCP/IP software is correctly installed and configured.

As the first and second layers of the ISO/OSI reference model are not included in the test, they should be tested separately using the ping function.

A 2.2 Value 255 in the Byte

Value 255 is defined as a broadcast address. The telegram is sent to all the PCs that are in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all the PCs in all the networks). If the network is divided into subnetworks, the subnet masks must be observed during calculation, otherwise some devices may be omitted.

0.x.x.x Addresses

Value 0 is the ID of the specific network. If the IP address starts with a zero, the receiver is in the same network. Example: 0.2.1.1 refers to device 2.1.1 in this network.

The zero previously signified the broadcast address. If older devices are used, unauthorized broadcast and complete overload of the network (broadcast system) may occur when using the IP address 0.x.x.x.

A 2.3 Subnet Masks

Routers and gateways divide large networks into several subnetworks. The subnet mask is used to assign the IP addresses of individual devices to specific subnetworks. The **network part** of an IP address is **not** modified by the subnet mask. An extended IP address is generated from the user address and subnet mask. Because the masked subnetwork is only recognized by the local PC, this extended IP address appears as a standard IP address to all the other devices.

Structure of the Subnet Mask

The subnet mask always contains the same number of bits as an IP address. The subnet mask has the same number of bits (in the same position) set to “one”, which is reflected in the IP address for the network class.

Example: A Class A IP address contains a 1-byte network address and a 3-byte PC address. Therefore, the first byte of the subnet mask may only contain 1s (ones). The remaining bits (three bytes) then contain the address of the subnetwork and the PC. The extended IP address is created when the bits of the IP address and the bits of the subnet mask are ANDed. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a “normal” IP address to all the other devices.

Application

If ANDing the address bits gives the local network address and the local subnetwork address, the device is located in the local network. If ANDing gives a different result, the data telegram is sent to the subnetwork router. Figure A-3 shows an example of a Class B subnet.

Figure A-3 Example for a Class B Subnet Mask

A 2.4 Examples for Subnet Masks and Computer Bits

See Table A-3.

Table A-3 Examples for Subnet Masks and Computer Bits

Subnet Mask	Computer/Host ID
255.255.255.252	2 Bits
255.255.255.248	3 Bits
255.255.255.240	4 Bits
255.255.255.224	5 Bits
255.255.255.192	6 Bits
255.255.255.128	7 Bits
255.255.255.0	8 Bits
255.255.254.0	9 Bits
255.255.252.0	10 Bits
255.255.248.0	11 Bits
...	...
...	...
255.128.0.0	23 Bits
255.0.0.0	24 Bits

B Appendices

B 1 List of Figures

Section 1

Figure 1-1: Features of the RAD-80211-XD wireless radio 1-4
Figure 1-2: Features of the RAD-80211-XD-BUS wireless radio 1-5
Figure 1-3: I/O Modules used with the RAD-80211-XD-BUS 1-6
Figure 1-4: Features of the RAD-80211-XD-WM wireless radio 1-7
Figure 1-5: Example of Access Point/Client 1-9
Figure 1-6: Example of Point-to-Point Bridging 1-10
Figure 1-7: Example of Bridge/Repeater Mode 1-10
Figure 1-8: Example of Point-to-Multipoint Bridging 1-11

Section 2

Figure 2-1: OMNI-directional and YAGI-directional Antenna Performance Characteristics 2-5

Section 3

Figure 3-1: Installation showing a DIN rail power supply, end clamps and ground terminal block 3-3
Figure 3-2: Installing and removing a module from the DIN rail 3-5
Figure 3-3: Typical installation of the RAD-80211-XD-WM radio 3-7
Figure 3-4: RAD-80211-XD-WM radio ground connection 3-7
Figure 3-5: RAD-80211-XD or RAD-80211-XD-BUS power connections 3-8
Figure 3-6: RAD-80211-XD or RAD-80211-XD-BUS transceiver wiring requirements 3-9
Figure 3-7: RAD-80211-XD-WM power connections 3-10
Figure 3-8: RAD-80211-XD-WM M12 cable connections 3-10
Figure 3-9: RS-232 wiring diagrams and pinouts 3-11
Figure 3-10: RS-422/485 2-wire and 4-wire connections 3-12
Figure 3-11: RAD-80211-XD-WM 2-wire and 4-wire connections 3-13
Figure 3-12: RAD-80211-XD or RAD-80211-XD-BUS Redundant Antenna Connections 3-14

Section 4

Figure 4-1: “Internet Protocol (TCP/IP) Properties” dialog box 4-3
Figure 4-2: “Sign In” screen 4-4
Figure 4-3: “Home” screen showing configuration data 4-4
Figure 4-4: “General Device Information” screen 4-5
Figure 4-5: “Local Diagnostics” screen 4-6
Figure 4-6: “General Configuration” screen 4-7
Figure 4-7: “Operational Mode Configuration” screen 4-8
Figure 4-8: RAD-80211-XD LAN Configuration 4-9
Figure 4-9: “LAN - SNMP Configuration” screen 4-10
Figure 4-10: RAD-80211-XD DHCP Configuration 4-11
Figure 4-11: “Access Point Configuration” screen 4-12
Figure 4-12: Channel-center frequencies (GHz) for 802.11b/g 4-13
Figure 4-13: Channel-center frequencies (GHz) for 802.11a 4-14
Figure 4-14: Access Point Radio - Security” screen showing Static WEP options 4-15
Figure 4-15: “Access Point Radio - Security” screen showing 802.11i and WPA options 4-17
Figure 4-16: “Access Point Radio - MAC Address Filtering” screen 4-18
Figure 4-17: “Access Point Radio - Rogue AP Detection” screen 4-19
Figure 4-18: “Access Point Radio - Advanced Settings” screen 4-20
Figure 4-19: “Client Radio - Settings” screen 4-21
Figure 4-20: “Client Radio - Security” screen 4-22
Figure 4-21: “Passphrase and Encryption Method” screen 4-23
Figure 4-22: Passphrase and Encryption Method for WPA-EAP-TLS Screen 4-23
Figure 4-23: Entering Security Titles (New or Updated) 4-24
Figure 4-24: Selecting Encryption Method for WPA-EAP-TLS 4-24
Figure 4-25: “Bridge Radio - General” screen showing Manual Bridging options 4-25
Figure 4-26: “Bridge Radio - Settings” screen showing Auto Bridging options 4-26
Figure 4-27: “Bridge Radio - Settings” screen 4-27
Figure 4-28: “Bridge Radio - Settings” screen 4-29
Figure 4-29: “Bridge Radio - Security” screen 4-30
Figure 4-30: “Ethernet Ports Configuration” screen 4-32
Figure 4-31: “Serial Ports Configuration” screen 4-33
Figure 4-32: “Configuration - Password Modification” screen 4-34
Figure 4-33: “Configuration – Store Retrieve Settings” screen 4-35

Figure 4-34: "Home" screen with performance options in the left navigation column 4-36
Figure 4-35: "Maintenance… Software Updates" screen 4-37
Figure 4-36: "Home" screen with monitoring/report options in the left navigation column 4-38

Section 5

Figure 5-1: "PLC Configuration" screen 5-5
Figure 5-2: Example of SNMP diagnostic error message 5-6
Figure 5-3: Error message – Multiple I/O communication control sources on same channel 5-7
Figure 5-4: I/O modules used with the RAD-80211-XD-BUS 5-8
Figure 5-5: I/O module 8-position rotary switch 5-15
Figure 5-6: RAD-IN-4A-I Analog Input Module wire diagram 5-18
Figure 5-7: RAD-IN-8D Digital Input Module wire diagram 5-19
Figure 5-8: RAD-OUT-4A-I Analog Output Module wire diagram 5-20
Figure 5-9: RAD-IN-OUT-8D-REL Digital Output Module wire diagram 5-21
Figure 5-10: RAD-OUT-8D-REL Digital Output Module wire diagram 5-22
Figure 5-11: RAD-IN-2D-CNT Pulse Input Module wire diagram 5-23
Figure 5-12: Description of RAD-IN-2CNT Digital Pulse Input Module LEDs 5-25
Figure 5-13: RAD-OUT-2D-CNT Digital Pulse Output Module wire diagram 5-26
Figure 5-14: Description of RAD-OUT-2D-CNT Digital Pulse Output Module LEDs 5-27
Figure 5-15: Example of data display 5-28

Section 6

Figure 6-1: RAD-80211-XD and RAD-80211-XD-BUS LED locations 6-3
Figure 6-2: RAD-80211-XD-WM LED locations 6-4
Figure 6-3: RAD-80211-XD and RAD-80211-XD-BUS RSSI voltage strength check 6-5
Figure 6-4: RAD-80211-XD-WM RSSI voltage strength check 6-6
Figure 6-5: Voltage vs. Signal Strength 6-7

Section 7

Figure 7-1: RAD-80211-XD and RAD-80211-XD-BUS Transceiver Dimensions . 7-5
Figure 7-2: RAD-80211-XD-WM Transceiver Dimensions 7-5

Section 8

Figure 8-1: Parts and Assemblies for the RAD-80211-XD and RAD-80211-XD-BUS Radio 8-3

Figure 8-2: Parts and Assemblies for the RAD-80211-XD-WM Radio 8-5

Appendix A

Figure A-1: Location of Bits within the IP Address A-1

Figure A-2: Structure of IP Addresses A-3

Figure A-3: Example for a Class B Subnet Mask A-5

Appendix B

B 2 List of Tables

Section 1

Section 2

Table 2-1: Cable Types and Signal Loss (dB) 2-6

Section 3

Section 4

Table 4-1: Hardware and Firmware Updates 4-37

Section 5

Table 5-1: MODBUS Memory Map 5-10
Table 5-2: Modbus Pulse Memory Map 5-11

Section 6

Table 6-1: LED descriptions 6-3
Table 6-2: LED descriptions 6-4
Table 6-3: Expected Raw Data Throughput 6-7
Table 6-4: RAD-80211-XD... Troubleshooting Procedures 6-8

Section 7

Section 8

Table 8-1: RAD-80211-XD and RAD-80211-XD-BUS Part Listing 8-4
Table 8-2: RAD-80211-XD-WM Part Listing 8-5
Table 8-3: Accessories 8-6

Appendix A

Table A-1: Class Assignments A-2
Table A-2: Network and User Class Bit Assignments..... A-2
Table A-3: Examples for Subnet Masks and Computer Bits..... A-6

Appendix B

B 3 Explanation of Terms

802.11a	An IEEE wireless networking standard that specifies a maximum data rate of 54 Mbps, OFDM modulation and an operating frequency of 5GHz.
802.11b	An IEEE wireless networking standard that specifies a maximum data transfer rate of 11 Mbps, DSSS modulation and an operating frequency of 2.4GHz.
802.11g	An IEEE wireless networking standard that specifies a maximum data transfer rate of 54 Mbps, OFDM modulation and an operating frequency of 2.4GHz.
Access Point	A device that allows wireless-equipped computers and other devices to communicate with a wired network.
Ad-hoc	A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.
AES (Advanced Encryption Standard)	A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S. government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.
AES-CCMP	AES-Counter Mode CBC-MAC Protocol (AES-CCMP) is the encryption algorithm used in the 802.11i security protocol. It uses the AES block cipher, but restricts the key length to 128 bits. It incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point.
Bandwidth	The transmission capacity of a given device or network.
Beacon Interval	The time interval in milliseconds in which the 802.11 beacon is transmitted by the access point.
Bit	A binary digit.
Bridge	A device that connects two local area networks (LANs) or two segments of the same LAN that use the same protocol, such as Ethernet or Token-Ring.
Browser	An application program that provides a way to look at and interact with all the information on the World Wide Web.
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)	A method of data transfer that is used to prevent data collisions.
CTS (Clear To Send)	A signal sent by a wireless device, signifying that it is ready to receive data.
DNS - (Domain Name System [or Service or Server])	An Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet, however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Default Gateway	A device that forwards Internet traffic from your local area network.
DHCP (Dynamic Host Configuration Protocol)	A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time instead of assigning permanent IP addresses.
DNS (Domain Name Server)	The IP address of your ISP’s server which translates the names of websites into IP addresses.
Domain	A specific name for a network of computers.
DSSS (Direct Sequence Spread Spectrum)	Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.
DTIM (Delivery Traffic Indication Message)	A message included in data packets that can increase wireless efficiency.
DTIM Interval	The number of beacon intervals that broadcast and multicast traffic is buffered for a client in power save mode.
Dynamic IP Address	A temporary IP address assigned by a DHCP server.
Encryption	Encoding data transmitted in a network.
Ethernet	IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.
Firewall	A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.
Firmware	The programming code that runs a networking device.
Fragmentation	Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
FTP (File Transfer Protocol)	A protocol used to transfer files over a TCP/IP network.
Gateway	A device that interconnects networks with different, incompatible communications protocols.
Half Duplex	Data transmission that can occur in two directions over a single line, but only one direction at a time.
Hardware	The physical aspect of computers, telecommunications and other information technology devices.
HTTP (HyperText Transport Protocol)	The communications protocol used to connect to servers on the World Wide Web.
IEEE (The Institute of Electrical and Electronics Engineers)	An independent institute that develops networking standards.

Infrastructure	A wireless network that is bridged to a wired network via an access point.
IP (Internet Protocol)	A protocol used to send data over a network.
IP Address	The address used to identify a computer or device on a network.
IPSec (Internet Protocol Security)	A VPN protocol used to implement secure exchange of packets at the IP layer.
ISM band (Industrial Scientific Medical band).	A license-free portion of the spectrum open to all users.
LAN	The computers and networking products that make up your local area network.
Load Balancing	In an infrastructure wireless LAN, the access point (AP) is responsible for connecting mobile stations (STA) and wired stations. Each access point is assigned on one channel. Traditionally, a station selects the access point connection based on the received signal strength indicator (RSSI). This approach may cause all active mobile stations to connect to few access points, and lots of contentions/collisions will occur by the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol. Consequently, the total network throughput will be degraded. Contrarily, if all STAs can be equally distributed to all access points and the signal strength of any pair of STA and connected access point is still kept in an acceptable range, the spare bandwidth in wireless LANs (WLANs) will be utilized in a more efficient way.
MAC (Media Access Control) Address	The unique address that a manufacturer assigns to each networking device.
Mbps (MegaBits Per Second)	One million bits per second; a unit of measurement for data transmission.
Network	A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.
Node	A network junction or connection point, typically a computer or work station.
Packet	A unit of data sent over a network.
Passphrase	Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.
Ping (Packet INternet Groper)	An Internet utility used to determine whether a particular IP address is online.
Port	The connection point on a computer or networking device used for plugging in cables or adapters.
PPPoE (Point-to-Point Protocol over Ethernet)	A type of broadband connection that provides authentication (username and password) in addition to data transport.
PPTP (Point-to-Point Tunneling Protocol)	A VPN protocol that allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

RADIUS (Remote Authentication Dial-In User Service)	An AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations. It is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard. RADIUS was originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers, but later (1997) published as RFC 2058 and RFC 2059 (current versions are RFC 2865 and RFC 2866). The DIAMETER protocol is the planned replacement for RADIUS, but is still backwards compatible.
RTS threshold	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
Roaming	The ability to take a wireless device from one access point's range to another without losing the connection.
Router	A networking device that connects multiple networks together.
RTS (Request To Send)	A networking method of coordinating large packets through the RTS threshold setting.
Server	Any computer whose function in a network is to provide user access to files, printing, communications and other services.
SPI (Stateful Packet Inspection) Firewall	A technology that inspects every incoming packet of information before allowing it to enter the network.
Spread Spectrum	Wideband radio frequency technique used for more reliable and secure data transmission.
SSID (Service Set IDentifier)	Service Set ID is a network ID unique to a network. Only clients and access points that share the same SSID are able to communicate with each other.
Static IP Address	A fixed address assigned to a computer or device that is connected to a network.
Static Routing	Forwarding data in a network via a fixed path.
Subnet Mask	An address code that determines the size of the network.
Ethernet Switch	A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports.
TCP (Transmission Control Protocol)	A network protocol for transmitting data that requires acknowledgment from the recipient of data sent.
TCP/IP (Transmission Control Protocol/Internet Protocol)	A set of instructions PCs use to communicate over a network.
TKIP (Temporal Key Integrity Protocol)	TKIP is a protocol used in WPA. It scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

UDP (User Datagram Protocol)	A network protocol for transmitting data that does not require acknowledgment from the recipient of the data that is sent.
VPN (Virtual Private Network)	A security measure to protect data as it leaves one network and goes to another over the Internet.
WAN (Wide Area Network)	A network that provides communication services between devices in a geographic area larger than that served by a local area network or a metropolitan area network. A WAN may use or provide public communication facilities.
WEP (Wired Equivalent Privacy)	A method of encrypting network data transmitted on a wireless network for greater security.
WINS - (Windows Internet Naming Service)	A system that determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. Determining the IP address for a computer is a complex process when DHCP servers assign IP addresses dynamically. For example, it is possible for DHCP to assign a different IP address to a client each time the machine logs on to the network. INS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
WLAN (Wireless Local Area Network)	A group of computers and associated devices that communicate with each other wirelessly.
WPA (Wi-Fi Protected Access)	A wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.